

The Power of Dark Data - Exploring the Role of Data Governance

Fatime Atta AlKhatib

**A thesis submitted in partial fulfilment of the requirements of the
University of East London for the degree of Doctor of Philosophy**

December 2024

Abstract

Holistic Dark Data Governance is an emerging field reshaping how organisations manage and govern their data. Despite significant investments in digital transformation, many organisations and institutions still struggle to adopt effective dark data governance practices. In Texas, USA, universities have made substantial investments in digital initiatives to keep pace with the rapidly evolving technological landscape in higher education. A considerable portion of these investments have been directed toward managing dark data, improving data quality, governance, and integration, and adopting modern applications to enhance educational outcomes. However, the challenge of dark data governance is not confined to Texas; it is a global issue that remains under-researched and infrequently practiced. This research represents a pioneering effort to tackle the challenge of dark data governance at one of the leading universities in Texas. By advancing research in this emerging field, the study proposes comprehensive methods for deploying effective holistic dark data governance models within the university setting, enabling the institution to better manage and control dark data, and thereby achieve its operational and strategic goals. The study began with an analysis of existing data governance frameworks, revealing their limitations due to a lack of focus on dark data. In response, this research aims to develop a holistic model designed to establish, deploy, and sustain effective dark data governance systemic functions within the organisational Viable System Model (VSM) context. The proposed framework offers a comprehensive approach to addressing the challenges of dark data governance, surpassing the limitations of traditional data governance frameworks. Additionally, it equips universities with the knowledge and tools necessary to implement such models, empowering them to manage and control dark data effectively to achieve their objectives. A crucial step in developing the proposed model was understanding the systemic functions of holistic data governance. To support the model's conceptualization, the study employed Critical Success Factors, VSM, and Cybernetics theories. Given the complexity of the model, organisations and institutions need a method to assess their current state and define their requirements. To facilitate this, the research introduced a Maturity Model alongside an Assessment Matrix. These tools were validated and evaluated at a top university in Texas using mixed research methods, including both qualitative and quantitative approaches. The Delphi approach was used for validation, with expert representation from the university. The Assessment Matrix evaluation enables organisations and institutions to determine their maturity levels in holistic dark data governance and define

the requirements for achieving their full viable level. To further assess the research findings and develop an improvement roadmap, the study incorporated a practical evaluation that examined the application of the assessment matrix across realistic case scenarios at three prominent universities in Texas, USA. These universities were actively implementing general data governance practices but had not yet adopted a comprehensive approach to dark data governance. This research significantly contributes to the academic debate on holistic dark data governance while offering practical frameworks that empower organisations and institutions to enhance their holistic data governance practices and achieve their operational and strategic goals.

Keywords: Data governance, Dark Data, Dark Data Governance, Holistic Dark Data Governance Model, Holistic Dark Data Governance Maturity Model, Holistic Dark Data Governance Maturity Assessment Matrix, Continuous Improvements, Viable System Model (VSM), Cybernetics

Acknowledgments

First and foremost, I am deeply grateful to Almighty Allah for granting me the strength and health that were essential in enabling me to complete this thesis.

I am deeply appreciative of my parents, Mariam and Atta, for their unwavering love and inspiration that have guided me throughout this endeavour. Additionally, I extend my sincere gratitude to my husband, Kassem, and my beloved daughters, Sarah, Diana, Mariam, and Eman, whose steadfast support, patience, prayers, and encouragement have been invaluable in helping me complete this thesis. Furthermore, I would like to thank my brothers and sisters for their constant moral support during this journey.

I would like to express my deepest gratitude to my advisors, Professor Rabih Bashroush, Dr. Umaima Haider, and Dr. Saeed Sharif, for their support throughout my PhD journey. Their encouragement, vast expertise, and patience have been invaluable, and their guidance has been instrumental in the successful completion of this thesis. Additionally, I am sincerely thankful to my friends and colleagues for their ongoing support and counsel. I also extend my heartfelt thanks to the experts from key Texas universities in the USA, as their data greatly enriched the quality of my research and provided me with the opportunity to broaden my expertise and knowledge in academic research.

Dedication

I would like to dedicate the completion of my PhD thesis to:

My parents

My husband and children

My brothers and sisters

My friends and colleagues

Table of Contents

Abstract.....	II
Acknowledgments.....	IV
Dedication.....	V
List of Tables	XI
List of Figures	XIII
List of Abbreviations	XVI
Chapter 1. Introduction to This Study.....	1
1.1. Introduction	1
1.2. Understanding Dark Data and the Imperative for Governance	3
1.2.1. Definition of Dark Data.....	3
1.2.2 The Power of Dark Data and the Imperative for Governance.....	6
1.3. Understanding Data Governance in Mitigating Dark Data	10
1.3.1 Definition of Data Governance	11
1.3.2 Data Governance and Other Governance Domains	14
1.4 Research Problem Statement and Motivation	21
1.5 Aim and Objectives of the Study.....	25
1.6 Research Questions.....	27
1.7 Research empirical context and background - Leading Universities in Texas, USA) ...	27
1.8 Research Contributions to Knowledge	29
1.9. Structure of the Thesis.....	31
Chapter 2. Methodology	34
2.1 Introduction	34
2.2 Aim and Objectives of the Study.....	34
2.3 Research Methodology	34
2.3.1. Research questions	34
2.3.2 Paradigms	35
2.3.3 Theoretical Frameworks.....	36
2.3.4 Research methods vs. methodology	36
2.3.5 Data collection and data sources	39
2.3.6 Time horizon	43
2.4 Validity and Reliability	43
2.5 Limitations.....	45

2.6 Ethical Considerations	47
2.7 Chapter Summary	48
Chapter 3. Tertiary Literature Review of Data Governance and Dark Data Governance	49
3.1. Introduction	49
3.2. Review Process Description	50
3.3. Tertiary Literature Review Questions	52
3.4. Inclusion and Exclusion Criteria	52
3.5. Defining the Review Protocol	53
3.6. Search Results and Study Selection.....	55
3.7. Results and Analysis.....	58
3.7.1. Publication Year.....	58
3.7.2. Nature of Contribution	60
3.7.3. Analysis of the State of the Art for Data Governance and Dark Data Governance	63
3.7.4 Analysis of Key Challenges	81
3.7.5. Analysis of Critical Success Factors	86
3.8 Critical Review Findings	92
3.9 Chapter Summary	95
Chapter 4. A Holistic Framework for Dark Data Governance	97
4.1. Introduction	97
4.2. Theoretical Foundation.....	98
4.2.1. Critical Success Factors (CSFs) Concept.....	99
4.2.2. The Viable System Model (VSM) Theories – based on Cybernetics and Systems Theories.....	100
4.3 VSM as a Holistic Governance Framework for Organisations	103
4.3.1. VSM Underlying Concepts	104
4.3.2. VSM Five Systems.....	105
4.3.3. VSM Communication Key Variety Loops.....	107
4.3.4. Key VSM communication channels.....	109
4.3.5. Key VSM Information Domains (Flows).....	111
4.4 Conceptualization of the Holistic Dark Data Governance Key Systemic Functions ...	119
4.4.1. VSM Underlying Concept and the Relevance to Holistic Dark Data Governance Context: Viability	120
4.4.2. Holistic Dark Data Governance Key Systemic Functions	121
4.5 Definitions of a Holistic Model for Dark Data Governance	145

4.5.1. Aim of the Model	145
4.5.2. Analysis of Existing Data Governance	146
4.6. Conceptualization of the Holistic Dark Data Governance Model	148
4.7. Methodology to Identify, Deploy, and Sustain the Proposed Model	151
4.7.1 Performative Process Description of a VSM Epistemology	151
4.7.2 The Methodology of Diagnosis and Design by VSM	153
4.7.3 Cycle of the VSM Methodology to diagnose an organisation	154
4.7.4 Methodology to identify, deploy, and sustain the HDGM	157
4.8. The Roadmap to Manage the Deployment and Sustainability of HDGM	164
4.9. Chapter Summary	166
Chapter 5: Holistic Dark Data Governance Maturity Model and Assessment Matrix	167
5.1. Introduction	167
5.2. Findings from the Literature Review on Maturity Models	169
5.3. Holistic Dark Data Governance Maturity Model	171
5.4. Dark Data Governance Maturity Model Development	173
5.4.1. Pre-Design Phase	174
5.4.2. Design Phase	175
5.4.3. Post-Design Phase	184
5.5. Assessment Matrix	185
5.5.1. Development of the Holistic Dark Data Governance Assessment Matrix	187
5.5.2. Structure of Implementing and Utilizing the Assessment Matrix	199
5.6. Chapter Summary	200
Chapter 6. Validation of the Holistic Dark Data Governance Model	202
6.1. Introduction	202
6.2. Design of the Validation Approach	202
6.3. Panel of Experts Validation Scope	205
6.3.1. Research Problem vs. Validation Scope of the Proposed Model	205
6.3.2. Experts' Feedback Description and Analysis	206
6.3.3 Deliverables	207
6.4. Participant Profiles	208
6.5. Data Analysis	209
6.5.1. Proposed Model Design Validation	210
6.5.2. Model Systemic Phases Validation	213

6.5.3. Validate the Systemic Functions Components of the Model Phases	216
6.5.4. Validation Results of the Model's Usability	224
6.5.5. Findings and Discussion.....	227
6.5.6. Overall Validation of the Proposed Model and Suggestions for Model Improvements.....	229
6.5.7. Model Refinement.....	232
6.6. Chapter Summary	237
Chapter 7: Evaluation of the Dark Data Governance Maturity Model and Maturity Assessment Matrix.....	238
7.1. Introduction	238
7.2. Design of the Validation Approach	239
7.3. Panel of Experts Validation Scope	239
7.4. Assessment Criteria	240
7.5. Evaluation of Holistic Data Governance Maturity Model and Assessment Matrix	241
7.6. Deliverables.....	243
7.7. Participants' Profiles.....	243
7.8. HDG Maturity Model Evaluation.....	245
7.8.1. Completeness	246
7.8.2. Consistency	246
7.8.3. Practicality.....	247
7.8.4. Usefulness	248
7.8.5. Verifiability.....	248
7.8.6. Participants' Recommendations to Improve the Proposed Maturity Model	250
7.9. Holistic Dark Data Governance Assessment Matrix Evaluation.....	252
7.9.1. Completeness	253
7.9.2. Consistency	254
7.9.3. Practicality.....	254
7.9.4. Usefulness	256
7.9.5. Verifiability.....	256
7.9.6. Strengths and Weaknesses	257
7.9.7. Participants' Recommendations to Improve the Proposed Assessment Matrix....	263
7.10. Practical Evaluation of the Research Findings	271
7.10.1. Case Scenario 1: University X	272
7.10.2. Case Scenario 2: University Y	274

7.10.3. Case Scenario 3: University Z.....	276
7.11. Chapter Summary	278
Chapter 8: Research Conclusions and Recommendations.....	279
8.1. Introduction	279
8.2. Research Overview.....	279
8.3. Summary of the Key Research Findings and Contributions	281
8.4. Research Limitations	284
8.5. Recommendations for Future Research.....	286
References.....	288
Appendices.....	303
Appendix A: Key Dark Data Types & their Description	303
Appendix B: UEL-Approved Ethical Forms	305
Appendix C: Analysis of Key Challenges for Data Governance Implementation	311
Appendix D: Analysis of Key Challenges for Dark Data Governance Implementation....	316
Appendix E: Analysis of Critical Success Factors (CSFs) for Data Governance Implementation.....	320
Appendix F: Analysis of Critical Success Factors (CSFs) for Dark Data Governance Implementation.....	325
Appendix G: Consolidated Critical Success Factors (CSFs) for Dark Data Governance Implementation.....	330
Appendix H: The Viable System Model’s Symbols (Adapted from Beer, 1985).....	338
Appendix I: Data Governance Domains - Key Descriptions	339
Appendix J: VSM Qualities vs. Assessment of Different Key Governance Models	341
Appendix K: VSM Qualities vs. Assessment of Key Industry Governance Models	348
Appendix L: The Methodology of Diagnosis and Design by VSM.....	352
Appendix M: Literature Review of HDG - Maturity Model (HDG-MM)	354
Appendix N: HDG Model Validation	369
Appendix O: Maturity Model & Assessment Matrix Evaluation.....	378
Appendix P: Practical Evaluation Results – Recommendations for Improvements	390

List of Tables

Table 1. 1 Key Dark Data Definitions	5
Table 1. 2 Key Dark Data Types	5
Table 1. 3 Data/Information Governance Definitions	12
Table 1. 4 The key contributions of this research to knowledge	30
Table 2. 1 Delphi three data collection rounds to validate HDGM	41
Table 2. 2 Delphi three data collection rounds to validate HDG-MM and HDG-MAM.....	42
Table 3. 1 Review Questions and Motivation.....	52
Table 3. 2 Inclusion and exclusion criteria for the tertiary review	53
Table 3. 3 Database of sources used for searching academic literature.....	55
Table 3. 4 Categorization of sources on data governance as per search protocol	58
Table 3. 5 The main findings of each Source	73
Table 3. 6 DG domains including domain decisions and potential roles.....	75
Table 3. 7 Key Challenges for Data Governance Implementation	84
Table 3. 8 Key Challenges for Dark Data Governance Implementation	86
Table 3. 9 Critical Success Factors (CSFs) for Data Governance Implementation.....	88
Table 3. 10 Critical Success Factors (CSFs) for Dark Data Governance Implementation.....	90
Table 3. 11 Dark Data Governance CSFs	91
Table 4. 1 Key VSM communication channels	110
Table 4. 2 Key VSM information domains (flows)	115
Table 4. 3 Key VSM Information Domains (Flows) within the VSM Systemic Context.....	117
Table 4. 4 The Key Systemic Functions of a Holistic Data Governance (HDG)	144
Table 4. 5 Constitutive Rules for an Interpretive VSM Methodology	152
Table 4. 6 Performative process description of VSM epistemology.	153
Table 4. 7 The Methodology of Diagnosis and Design by VSM.....	154
Table 4. 8 Methodology to Identify, Deploy, and Sustain HDGM.....	163
Table 5. 1 Maturity Models Literature Review Questions	169
Table 5. 2 Description of the three-phase Approach used to construct the dark data governance Maturity Model.....	174
Table 5. 3 HDG -Dimensions and their respective sub-dimensions.....	182

Table 5. 4 Maturity levels and their descriptions.....	184
Table 5. 5 Critical considerations to distinguish between the maturity levels in the maturity matrix	189
Table 5. 6 HDG-MD1 Assessment Matrix	191
Table 5. 7 HDG-MD2 Assessment Matrix	195
Table 5. 8 HDG-MD3 Assessment Matrix	199
Table 6. 1 Research questions versus the validation Scope of the Proposed Model	206
Table 6. 2 The demographic characteristics of the participants.....	208
Table 6. 3 The consensus and means of the participants’ feedback on the statements to validate the model design.....	211
Table 6. 4 The consensus and means of the participants’ feedback on the validation of the model phases	215
Table 6. 5 The mean and consensus% of the participants’ feedback on the SFs of phase 1 .	217
Table 6. 6 The mean and consensus% of the participants’ feedback on the SFs of Phase 2.	220
Table 6. 7 The mean and consensus% of the participants’ feedback on the SFs of Phase 3.	223
Table 6. 8 The consensus and means of the participants’ feedback on the statements to validate the model usability	226
Table 6. 9 The results of the investigation by the participants	230
Table 6. 10 The improvements suggested by the participants	231
Table 6. 11 Amended model (HDGM) after participants' feedback.....	236
Table 7. 1 The demographic characteristics of the participants.....	245
Table 7. 2 Amended maturity levels’ description after participants' feedback.....	251
Table 7. 3 Amended HDG-MD1 Assessment Matrix after participants' feedback.....	265
Table 7. 4 Amended HDG-MD2 Assessment Matrix after participants' feedback.....	268
Table 7. 5 Amended HDG-MD3 Assessment Matrix after participants' feedback.....	271
Table 7. 6 The maturity level of holistic dark data governance in University X.....	273
Table 7. 7 The maturity level of holistic dark data governance in University Y.....	275
Table 7. 8 The maturity level of holistic dark data governance in University Z	277

List of Figures

Figure 1. 1 How valuable is data to Organisations (Splunk., 2019)	7
Figure 1. 2 Dark Data in Organisations (Splunk., 2019)	7
Figure 1. 3 Data Governance is at the centre of all other governance domains (Olaitan, O., Herselman, M. and Wayi, N., 2016)	19
Figure 1. 4 Data Governance overlaps with IT Governance & Cloud Governance at the centre within the other governance domains (Al-Ruithe, M., 2018)	20
Figure 1. 5 Relationship between Corporate, IT, and Data Governance (Cheong, K. L. and Chang, V., 2007)	20
Figure 1. 6 Thesis Structure	33
 Figure 2. 1 The research onion (Zolfagharian, M. et al., 2019)	 35
 Figure 3. 1 The main process used to conduct the tertiary literature review	 55
Figure 3. 2 The selection process of Data Governance and Dark Data Governance Sources	56
Figure 3. 3 Distribution of Sources by Nature of Contribution	59
Figure 3. 4 The distribution of sources over the studied years	59
Figure 3. 5 The distribution of DG sources over the studied years for data governance	60
Figure 3. 6 The distribution of Dark DG sources over the studied years for dark data governance	61
Figure 3. 7 The number of all sources is based on the nature of the contribution.	62
Figure 3. 8 The number of Sources of data governance is based on the nature of the contribution.	62
Figure 3. 9 The number of sources of dark data governance based on the nature of the contribution.	63
Figure 3. 10 Contingency Approach to DG	74
Figure 3. 11 Data Governance Morphology – DG Goals and DG Structure	76
Figure 3. 12 Data Governance within Data Management Context (DAMA, 2017)	77
Figure 3. 13 Integrated Data Governance (intra- and inter-organisational) Context	78
Figure 3. 14 The DGI Data Governance Framework	78
Figure 3. 15 Dark Data Governance CSFs	92
 Figure 4. 1 Viable System Model (VSM) Recursivity	 106
Figure 4. 2 Key VSM Systemic Communication Channels	110
Figure 4. 3 VSM can be viewed as an Information System	111

Figure 4. 4 The Viable System Model (Adapted from Beer, 1985)	117
Figure 4. 5 VSM Dynamic Recursive Framework (e.g. two recursion levels).....	118
Figure 4. 6 HDGM Systemic Functions SF1 to SF5 within Organisational VSM Context ..	150
Figure 4. 7 HDGM Systemic Functions SF6 to SF11 within Organisational VSM Context	150
Figure 4. 8 The Methodology of Diagnosis and Design by VSM (Rezaee, Z. et al., 2018)..	154
Figure 4. 9 The cycle of the VSM Methodology to diagnose an organisation (Yolles, M., 2006)	156
Figure 4. 10 Methodology to Identify, Deploy, and Sustain the HDGM	164
Figure 4. 11 Roadmap to Manage the Deployment and Sustainability of HDGM.....	165
Figure 5. 1 Approach for constructing the dark data governance Maturity Model	173
Figure 5. 2 Holistic Dark Data Governance Maturity Model Architecture within the Organisational VSM Context.....	176
Figure 5. 3 Holistic Dark Data Governance Maturity Model Improvement Mechanisms within the Organisational VSM Context.....	177
Figure 5. 4 The Holistic Dark Data HDG Maturity Dimensions and Sub-Dimensions	180
Figure 5. 5 The dark data governance maturity levels within the organisational VSM context	183
Figure 5. 6 Phases and decision points of the roadmap to develop an assessment matrix. Source: (Maier et al., 2012)	186
Figure 5. 7 The structure to implement the holistic dark data governance assessment matrix.	200
Figure 6. 1 The balancing point for the accuracy of the framework.....	209
Figure 6. 2 The participants' feedback on the validation statements of the model design	210
Figure 6. 3 The consensus and means of the participants' feedback on the statements to validate the model design.....	212
Figure 6. 4 The participants' feedback on the validation of the model phases.....	213
Figure 6. 5 The participants' feedback on the validation of the model phases.....	215
Figure 6. 6 The participants' feedback on the SFs of Phase 1	216
Figure 6. 7 The participants' feedback on the validation of the SFs of Phase 1.....	218
Figure 6. 8 The participants' feedback on the SFs of Phase 2.....	218
Figure 6. 9 The participants' feedback on the validation of the SFs of Phase 2.....	221
Figure 6. 10 The participants' feedback on the SFs of Phase 3	222
Figure 6. 11 The participants' feedback on the validation of the SFs of Phase 3.....	224

Figure 6. 12 The participants' feedback on the validation statements of the model usability	225
Figure 6. 13 The consensus and means of the participants' feedback on the statements to validate the model usability	226
Figure 6. 14 The consensus percentage results of the model design	227
Figure 6. 15 The consensus percentage results of the model phases-SFs.....	228
Figure 6. 16 The consensus percentage results of the model usability	228
Figure 6. 17 Confirmed Model (HDGM) after Participants' Feedback.....	237
Figure 7. 1 The holistic dark data governance maturity model evaluation process.....	245
Figure 7. 2 The respondents' feedback for maturity model completeness	246
Figure 7. 3 The respondent's feedback on the maturity model's consistency	247
Figure 7. 4 The respondent's feedback on the maturity model's practicality.....	248
Figure 7. 5 The respondents' feedback on the maturity model's usefulness	249
Figure 7. 6 The respondent's feedback on the maturity model verifiability.....	249
Figure 7. 7 Amended dark data governance maturity after participants' feedback.....	251
Figure 7. 8 Amended maturity model after participants' feedback.....	252
Figure 7. 9 The holistic dark data governance assessment matrix evaluation process	253
Figure 7. 10 The respondents' feedback for assessment matrix completeness.....	254
Figure 7. 11 The respondents' feedback for assessment matrix consistency	255
Figure 7. 12 The respondents' feedback for assessment matrix practicality	255
Figure 7. 13 The respondents' feedback on the usefulness of the assessment matrix	256
Figure 7. 14 The respondents' feedback on the verifiability of the assessment matrix.....	257
Figure 7. 15 The scores for the content's strengths and weaknesses of the individual levels in the assessment matrix	258
Figure 7. 16 The consensus% for the content's strengths and weaknesses of the individual levels in the assessment matrix	259
Figure 7. 17 The scores for the strengths and weaknesses of the individual systemic function in the assessment matrix	260
Figure 7. 18 The consensus% for the strengths and weaknesses of the individual systemic function in the assessment matrix	261
Figure 7. 19 The assessment of dark data governance in University X.....	274
Figure 7. 20 The assessment of dark data governance in University Y.....	276
Figure 7. 21 The assessment of dark data governance in University X.....	278

List of Abbreviations

HDG	Holistic Data Governance
HDGM	Holistic Data Governance Model
IT	Information Technology
DM	Data Management
IG	Information Governance
VSM	Viable System Model
CSFs	Critical Success Factors
DD-Type	Dark Data Type
DAMA	Data Management Association International
DGI	Data Governance Institute
UTIMCO	University of Texas & Texas A&M Investment Management Company
UNT	University of North Texas
TCU	Texas Christian University
DQM	Data Quality Management
SLA	Service Level Agreement
DSR	Design Science Research
CMM	Capability Maturity Model
RBV	Resource-Based View
CMMI	Capability Maturity Model Integration
GRC	Governance, Risk Management, And Compliance
PMMM	Project Management Maturity Model
COBIT	Control Objectives for Information and Related Technologies.
BI	Business Intelligence
KM	Knowledge Management
NIST	National Institute of Standards and Technology
SCM	Supply Chain Management

Chapter 1. Introduction to This Study

1.1. Introduction

In the era of information and digital transformation, data volume is projected to escalate dramatically. Academia often distinguishes data from information by characterizing data as raw, unprocessed facts, while information is described as data that has been contextualized or processed ([Huang, K., Lee, W. Y. and Wang, Y. R., 1999](#)), ([Price, R. and Shanks, G., 2004](#)), ([Weber, K., Otto, B. and Osterle, H., 2009](#)). This study will use the terms 'data' and 'information' interchangeably, in alignment with the predominant approaches employed in the relevant data and information governance literature ([Weber, K., Otto, B. and Osterle, H., 2009](#)). Due to the digital transformation evolution, new business models solely based on data are emerging within organisations. At the same time, data and information management are becoming very challenging and organisations are not able to handle the increasing complexities dictated by the digital transformation era. Henceforward, there is a critical need for enhanced ways to steer data handling and drive the new business demands of intelligent utilization of data and information within organisations and ensure the availability of good data. As a result of the ongoing digital transformation, organisations are adopting novel business models centred around data. Concurrently, the management of data and information has become increasingly challenging, and organisations struggle to address the growing complexities driven by the digital transformation era. Consequently, there is a critical need for enhanced approaches to direct data handling and drive the new business demands of intelligent data and information utilization within organisations, ensuring the availability of reliable data. According to IBM's estimates, the annual cost of poor data quality in the United States alone is a staggering \$3.1 trillion ([Redman, T., 2016](#)). Therefore, the success of the new business models must be based on good data since that data is becoming the competitive currency of digital transformation. Academics and industry professionals have started to realize the importance of managing and governing data to counteract bad data risks.

Consequently, the success of the emerging business models must be predicated on high-quality data, as data is becoming digital transformation's competitive currency. Academics and industry experts have begun to recognize the importance of managing and governing data to mitigate the risks posed by poor-quality data or Dark Data. Dark data refers to low-quality information that encompasses diverse types of inaccurate, incomplete, underutilized, inconsistent, distorted, or falsified data. Prior studies have established the substantial positive impact of effective data governance practices on enhancing data availability, increasing the

utilization and insights derived from organisational data, minimizing errors and inconsistencies within the data, and mitigating the significant risks posed by dark data - the low-quality, underutilized, or falsified information that can undermine organisational decision-making and performance. These benefits of robust data governance have been well-documented in academic literature and industry research. Although the importance of governing low-quality or "dark" data to achieve organisational goals is widely recognized, the field of dark data governance remains understudied and lacks a comprehensive and structured approach within the broader scope of data governance ([Hand, J. D., 2020](#)). There is a critical need to develop a more holistic and formal framework for dark data governance that is integrated within the overall data governance strategy of organisations. This would enable companies to better mitigate the substantial risks posed by dark data and leverage their data assets more effectively to support strategic objectives. The concept of data governance gained traction in the 1990s as organisations increasingly relied on data-driven decision-making and the internet revolutionized how data was collected, stored, and shared ([Weber, K., Otto, B. and Osterle, H., 2009](#)). Data governance involves the formal management of data assets within an organisation to ensure data accuracy, accessibility, and protection throughout its lifecycle. It encompasses a range of practices, including data stewardship, data quality management, and compliance with regulatory requirements ([Khatri, V. and Brown, C., 2010](#)). As data governance practices matured, they began to include not only the management of structured data but also unstructured data, which led to the emergence of a more specialized field known as "dark data governance." The concept of dark data governance has gained importance in recent years as organisations become more aware of the risks and opportunities associated with this type of data. Dark data governance focuses on identifying, managing, and leveraging this hidden data to mitigate risks, such as security breaches and compliance issues, and to uncover potential business insights ([Borne, K., 2014](#)).

The evolution of dark data governance can be seen as part of the broader trend towards holistic data governance, where organisations strive to integrate all forms of data into a unified governance framework. This approach is critical in the current digital landscape, where data volumes continue to grow, and the complexity of managing diverse data sources increases ([Zicari, V. R., 2014](#)). As organisations continue to recognize the strategic value of data, dark data governance is likely to play an increasingly important role in ensuring that all data, regardless of its origin or structure, is effectively managed and utilized to support organisational goals.

This chapter outlines the purpose of the study, defining key concepts such as dark data and data governance, which form the foundation of the research. It introduces the nature of dark data and the role of data governance, followed by a discussion of the research problem and motivations behind the investigation. The chapter then presents the study's specific aim, key objectives, and research questions. Additionally, it highlights the potential contributions to academic knowledge and concludes by providing an overview of the thesis structure and organisation.

1.2. Understanding Dark Data and the Imperative for Governance

This section provides an in-depth discussion of the definition of dark data and emphasizes the critical importance of implementing effective data governance practices to mitigate the risks associated with dark data and enable organisations to achieve operational efficiency and strategic goals.

1.2.1. Definition of Dark Data

There is no universal agreement on the definition of dark data within the academic literature and industry publications. The key definitions of dark data presented below (Table 1.1) illustrate its diverse and multifaceted nature, reflecting the range of challenges it presents to organisations. The lack of consensus on a single, clear definition underscores the complex and elusive nature of this phenomenon. Despite the absence of a universally accepted definition, the various perspectives and conceptualizations of dark data provide a more holistic understanding of this concept and the challenges it poses for organisations.

Definition	Reference
Hand D.J. postulated that dark data exhibit similarities to dark matter in physics. Analogous to how dark matter cannot be directly observed yet exerts a powerful gravitational influence on visible matter in the universe, dark data are often invisible or difficult to measure, yet they can significantly impact an organisation's decisions and actions. Like dark matter, dark data often comprise a substantial portion of an organisation's information assets, but remain hidden, underutilized, and underappreciated. Despite their unseen nature, dark data can have serious consequences on an organisation's operations, performance, and strategic objectives if left unmanaged. Just as the presence of dark matter shapes the structure and evolution of galaxies, the existence of	Hand, D.J., 2020

Definition	Reference
dark data can shape and distort an organisation's decision-making and data-driven initiatives if not properly identified and governed. Hand also provided a comprehensive classification of fifteen distinct types of dark data (Table 1.2), as explained in Appendix A for further reference. Additionally, organisations must proactively recognize and manage the phenomenon of dark data to avoid potential risks, missed opportunities, and potentially disastrous consequences. The risks associated with dark data may be escalating. While the capacity to rapidly accumulate large datasets and leverage advanced analytics tools presents significant potential benefits, these advancements also introduce challenges. As data-driven decision-making becomes increasingly pervasive, the dangers posed by dark data, including security vulnerabilities, compliance breaches, and lost business opportunities, become increasingly salient. Similar to dark matter in physics, dark data often comprise most organisations' universe of information assets. Consequently, organisations frequently retain dark data for compliance purposes only, despite the fact that storing and securing data typically incurs more expense than value.	
According to Gartner, dark data refers to the information assets that organisations accumulate, process, and store during routine business operations, but typically do not leverage for additional purposes like analytics, insights, and direct monetization. This vast collection of underutilized data often remains hidden and untapped, representing a significant missed opportunity for organisations to derive value from their information assets.	Gartner, 2020
Other researchers defined dark data as unstructured data that does not get analysed. It's the data stored through various network processes on servers and in data lakes that ends up sitting around to satisfy the industry's regulations or is kept because data storage can be so cheap.	Cheng, S., 2018
Researchers have defined dark data in various ways. Some have characterized it as missing, not utilized, partially visible, poor, dirty, bad, low-quality, or corrupted data. These differing definitions highlight the multifaceted and complex nature of dark data and the challenges organisations face in identifying and managing this type of underutilized information asset.	Veaux, D.D.R. and Hand, J.D., 2005; Ajis, M.F.A. and Baharin, H.S., 2019; Gimpel, G., 2020; Wiebe, H.P. and Allison, D.M., 2015; Redman, C.T., 2018;

Definition	Reference
	Provost, J. and Danyluk, A., 1995

Table 1. 1 Key Dark Data Definitions

Hand D.J. provided a classification of fifteen distinct types of dark data, as illustrated in Table 1.2, the description of each type is provided in Appendix A for further reference.

ID	Dark Data Type
1	Data We Know Are Missing (Known Unknowns)
2	Data We Don't Know Are Missing (Unknown Unknowns)
3	Choosing just some data cases
4	Self-selection in supplying data
5	Missing What Matters especially the confusion between data correlation and data causation
6	Data that might have been
7	Data when changes with time
8	Definitions of Data especially inconsistencies
9	Summaries of Data (details are lost)
10	Data Measurement Error and Uncertainty
11	Feedback and Gaming – impact on data gathering especially bias
12	Information Asymmetry
13	Intentionally Darkened Data
14	Fabricated and Synthetic Data
15	Extrapolating beyond existing data

Table 1. 2 Key Dark Data Types

The definitions of dark data present diverse perspectives, reflecting its multifaceted and complex nature. Gartner (2020) adopts a practical, business-centric approach, defining dark data as underutilized information assets accumulated during routine operations, emphasizing the missed opportunities for analytics, insights, or monetization. In contrast, Hand (2020) uses a metaphorical lens, comparing dark data to dark matter in physics—unseen yet highly influential—and highlighting its significant risks to organisational decisions, security, compliance, and strategic objectives. Cheng (2018) provides a technical perspective, focusing on dark data as unstructured information often stored for regulatory purposes or due to low storage costs. Additionally, multiple authors (Veaux et al., Ajis et al., Gimpel, Wiebe et al., Redman, Provost, and Danyluk) characterize dark data in various ways, including missing, underutilized, low-quality, or corrupted data, emphasizing the challenges organisations face in identifying and managing it effectively. While Gartner and Hand focus on untapped potential

and systemic risks, Cheng emphasizes regulatory drivers, and the broader literature highlights the diverse dimensions and governance challenges associated with dark data. Together, these definitions underscore the critical need for organisations to address dark data's risks and opportunities.

This study will propose a novel definition of dark data in Chapter 4 (Section 4.5) that reflects the multifaceted nature and context of dark data described above. The proposed definition will aim to capture the significant influence and impact of dark data on an organisation's goals and decision-making processes. Additionally, it will provide direction for the purpose and scope of this research inquiry into dark data governance.

1.2.2 The Power of Dark Data and the Imperative for Governance

Organisations accumulate vast amounts of data as part of their operational and strategic requirements. However, as time progresses, a significant portion of this data becomes neglected within the organisation's data repositories without undergoing analysis or further processing, often due to constraints in financial and human resources or time ([Weber, K., Otto, B. and Osterle, H., 2009](#)). Unclear policies pertaining to the data lifecycle, from acquisition to disposal stages, cultivate the phenomenon known as dark data, with estimates indicating that over 50% of enterprise data remains unanalysed and underutilized ([Marus, P., 2018](#)). Most organisations focus on managing their tangible assets, such as physical infrastructure and equipment, while overlooking the substantial value inherent in their data assets ([Olaitan, O., Herselman, M. and Wayi, N., 2016](#)). Organisations consistently acknowledge the importance of data as an organisational asset, yet they persistently fail to fully realize and leverage the inherent value of this informational resource ([Nagle, T. and Sammon, D., 2017](#)). Daily organisational decisions necessitate data, but accessing and processing this information can be time-consuming and resource-intensive. The data needed often contains errors, and due to pressing deadlines, many employees choose to make their own corrections to complete tasks rather than reaching out to the original data creators. This failure to collaborate and address the root causes of data quality issues results in the proliferation of a "hidden data factory" - a reactive, piecemeal approach to data management that compounds inefficiencies ([Redman, T., 2016](#)).

According to Veritas, 33% of enterprise data remains unutilized ([Marus, P., 2018](#)). Halliburton further emphasized that the voluminous information collected far exceeds human cognitive capacity, with advancements in sensor technology leading to substantial accumulation of both dark data and what he refers to as "bright data" - data with untapped potential ([Deloitte, P. U., 2017](#)). Despite global recognition of data's value in driving organisational success, efficiency,

and profitability, as shown in Figure 1.1 ([Splunk., 2019](#)), organisations often fail to recover dark data and mitigate associated risks. In fact, 60% of organisations report that half or more of their data is dark, as illustrated in Figure 1.2 ([Splunk., 2019](#)).

The presence of dark data can lead organisations to undervalue and overlook their existing data assets, especially when that data is of questionable quality or “known unknowns” or “unknown unknowns” ([Hand, J. D., 2020](#)). While the risks posed by dark data have long been recognized, the proliferation of large-scale data collection and the increasing sophistication of analytical tools like AI and machine learning may be worsening these challenges ([Hand, D., 2020](#)).

How valuable is data to each of the following? <i>Showing % of extremely + very valuable</i>	GLOBAL	UNITED STATES	UNITED KINGDOM	FRANCE	GERMANY	CHINA	JAPAN	AUSTRALIA
Your organization's overall success	81%	86%	85%	64%	76%	82%	73%	81%
Your organization's efficiency	81%	85%	89%	68%	77%	78%	72%	81%
Your organization's profitability	78%	82%	79%	63%	75%	77%	75%	84%

Figure 1. 1 How valuable is data to Organisations (Splunk., 2019)

% of respondents reporting that ...	GLOBAL	UNITED STATES	UNITED KINGDOM	FRANCE	GERMANY	CHINA	JAPAN	AUSTRALIA
75% or more of their organization's data is dark	33%	36%	33%	42%	26%	15%	35%	36%
Half or more of their organization's data is dark	60%	63%	63%	65%	58%	44%	65%	62%
Less than half of their organization's data is dark	40%	37%	37%	35%	42%	56%	35%	38%
Less than 25% of their organization's data is dark	11%	11%	9%	11%	14%	9%	15%	10%

Figure 1. 2 Dark Data in Organisations (Splunk., 2019)

In the machine learning domain, the selection of poor-quality data can impede profitable business outcomes. This is due to the detrimental impact of bad data, manifesting in two ways: first, in the historical data used to train the predictive model, and second, in the new data employed by the model to inform future decisions ([Redman, C. T., 2018](#)). Even small amounts of poor-quality data can be crucial in understanding a situation, despite claims that large volumes of data may mask errors from minor missing values. For example, an algorithm trained on data lacking information about a rare but fatal disease would produce inaccurate diagnoses for patients with that condition. The key question for organisations is whether these small data gaps matter, and if the push towards data-driven decision-making is worsening the problem ([Hand, J. D., 2020](#)). Dark data can have catastrophic consequences, and it is not solely an issue

associated with large data sets. For instance, the 1986 Challenger space shuttle disaster, which resulted in the loss of a \$3 billion vehicle and the tragic deaths of all seven crew members, was exacerbated by decision-makers' lack of awareness regarding critical missing data in their analysis. In this case, the decision to launch the shuttle at a temperature well below any previously documented experience was made without a full understanding of the relevant data, demonstrating the dangers of extrapolating beyond the known data set ([Hand, J. D., 2020](#)), ([Bell, E. T. and Esch, K., 2016](#)). The Chernobyl nuclear disaster of 1986, which occurred in northern Ukraine, is considered the world's worst nuclear power catastrophe. It was caused by an incompetent team conducting a flawed experiment on a reactor with a faulty design, the details of which were unknown to them. The resulting reactor explosion released radioactive materials that spread across Europe and a large part of the globe, impacting an estimated seven million people and incurring billions of dollars in remediation efforts ([Ray, M., 2024](#)).

The causes of poor-quality and dark data are numerous, stemming from various stages of the data life cycle. Data can become distorted or corrupted during initial collection, recording, transfer, analysis, transformation, merging, copying, or through the introduction of new non-descriptive and inconsistent definitions over time. ([Veaux, D. D. R. and Hand, J. D., 2005](#)). The accumulation of dark data within organisations can be attributed to the various challenges encountered in conducting strategic and day-to-day business activities, both internally and across the broader ecosystem of partners, suppliers, and customers. Organisations encounter challenges in addressing dark data as a threat to their continued operation or an institutional problem. These obstacles include the substantial volume of dark data, a lack of necessary skill sets and resources, difficulties in coordinating across internal departments and with external data-generating parties, limited control over data-generating devices and applications, disinterest from organisational leadership, insufficient creativity, unawareness of data locations or even the existence of data, lack of clear accountabilities and policies, inadequate information governance ([Splunk., 2019](#)), ([Schembera, B. and Durán, M. J., 2020](#)), ([Purss, B. M. et al., 2015](#)), ([Ajis, M. F. A. and Baharin, H. S., 2019](#)).

Dark data can have a profound impact on organisational conclusions, decisions, and actions. Dark data poses a critical risk that organisations cannot afford to overlook, as it can be considered an organisational pathology that threatens the very survival of any institution ([Hand, J. D., 2020](#)). By failing to recognize the power of dark data, organisations risk falling behind in an increasingly data-centric business environment, where those who effectively manage and harness all forms of data will thrive ([Hand, J. D., 2020](#)). Therefore, addressing dark data is not merely a matter of optimizing storage and costs; it is critical to maintaining a competitive edge,

ensuring compliance, and protecting the organisation from significant security risks. Unmanaged and unmonitored data may include sensitive or proprietary information, which can become a target for cyberattacks if left unprotected. Studies have shown that breaches often occur due to overlooked data that is not adequately governed, leading to compliance issues and regulatory fines, especially under frameworks such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) ([Curry, E., Hasan, S. and Donnellan, B., 2018](#)). In addition to security concerns, dark data can lead to inefficiencies and missed opportunities within organisations. When critical data remains hidden, it restricts the ability to gain comprehensive insights, thereby limiting the effectiveness of predictive analytics, market trend identification, and overall decision-making ([Borne, K., 2014](#)). Organisations that fail to leverage dark data may find themselves at a competitive disadvantage, unable to fully exploit data-driven innovations such as artificial intelligence and machine learning, which depend heavily on the breadth and quality of available data ([Eckerson, W. W., 2017](#)).

According to the preceding analysis, unmanaged dark data presents considerable risks and missed opportunities for organisations. There is a growing understanding from executives that high-performance organisations use more than their gut feel to make decisions by using real data to set business directions. The main reason behind gut decisions within organisations is dark data since good data is not available. For better decisions to meet business goals, data management strategies and data governance need to be improved ([Sarsfield, S., 2009](#)). Another reason why dark data must be given a high priority is that organisations could easily become victims of legal battles if their data is found to be dark: deceptive, unrepresentative of the truth or has been fabricated in any way. The only way to minimize and contain such risk is by ensuring data is governed from the root ([Olaitan, O., Herselman, M. and Wayi, N., 2016](#)). Hence, unaddressed data issues can cause organisations financial implications in addition to the penalties for noncompliance. Such risks can be fixed by establishing data governance ([Sarsfield, S., 2009](#)). Data governance can be a long-term strategic solution for dark data and information availability issues, and other performance issues while organisations are trying to achieve their business goals ([Sarsfield, S., 2009](#)). The lack of governance around dark data complicates data management, as organisations risk making critical decisions based on incomplete or outdated information ([Redman, T., 2016](#)). Research emphasizes that Data governance can mitigate these risks by implementing policies, procedures, and accountability structures to ensure data is collected, stored, managed, and utilized in alignment with the organisation's strategic objectives and legal obligations ([Khatri, V. and Brown, C., 2010](#)). A

lack of data governance leaves organisations ill-equipped to meet these requirements, exposing them to penalties and legal ramifications ([Deloitte., 2020](#)). Inadequate management of dark data can result in biased insights, suboptimal decision-making, and reduced responsiveness to emerging trends or disruptions. Experts in this field have emphasized that without formal data governance, although the chaos may not be immediately apparent, the situation is effectively out of control. The indicators are readily observable, such as dirty data, redundant data, inconsistent data, integration challenges, poor performance, inadequate data availability, and limited accountability ([Al-Ruithe, M., 2018](#)). In addition to the potential benefits of effective data governance, there are also risks associated with the absence or inadequacy of data governance approaches. Data governance is widely recognized within organisations as a promising strategy to mitigate the risks posed by dark data, and it is regarded as a critical success factor for leveraging data assets to deliver business value and achieve strategic objectives ([Marus, P., 2018](#)), ([Hand, J. D., 2020](#)), ([Deloitte, P. U., 2017](#)), ([Al-Ruithe, M., Benkhelifa, E. and Hameed, K., 2018](#)), ([DAMA., 2017](#)). In the long run, organisations that fail to govern dark data effectively are likely to face escalating challenges that undermine their operational efficiency, goal attainment, compliance maintenance, and security profile.

The subsequent sections will provide a comprehensive exploration of the critical role of data governance in addressing the significant risks and challenges posed by dark data within organisations (Section 1.3.). This discussion will delve deeper into the research problem and the fundamental necessity for a novel, holistic data governance model that can effectively mitigate the undesirable impacts of dark data and optimize its management across the broader organisational context (Section 1.4.).

1.3. Understanding Data Governance in Mitigating Dark Data

Understanding data governance is essential for counteracting dark data, which refers to structured, unstructured, unused, low-quality, or unmanaged data that organisations collect but fail to exploit for business insights and achievement of their goals. The dark data phenomenon is becoming increasingly prevalent as the volume of data collected by businesses continues to grow exponentially. According to IDC, approximately 90% of all digital data generated goes unused or unanalysed, leading to significant untapped potential ([IDC., 2018](#)). Dark data often includes information stored in databases, emails, logs, customer records, and other digital repositories that are not actively analysed or integrated into decision-making processes ([Gartner., 2020](#)). Dark data represents a considerable portion of the digital universe and poses both challenges and opportunities for organisations. While it includes various forms of

structured and unstructured data, the failure to exploit this data can lead to inefficiencies, non-compliance, and missed opportunities. Therefore, robust data governance implementations are critical for mitigating the risks associated with dark data and unlocking its potential to generate valuable business insights and support the achievement of organisational objectives. Data governance is especially pivotal when addressing dark data, which poses significant challenges such as compliance breaches, security vulnerabilities, and operational inefficiencies stemming from data proliferation ([Gartner., 2020](#)). Section 1.3.1. provides a discussion on the definition of data governance.

1.3.1 Definition of Data Governance

The academic literature and industry publications do not present a single, universally accepted definition of data governance among researchers and practitioners. Instead, the definitions of data governance vary considerably, reflecting the diverse perspectives and specialized interests of different professionals and scholars. As a result, there is no official, comprehensive definition that captures the full breadth of this domain. To establish an appropriate definition for the purposes of this study, the author reviewed and evaluated multiple definitions presented in academic literature and industry sources. Key diverse conceptualizations of data governance are summarized and highlighted in Table 1.2.

	Authors	Data/Information Governance Definition
1	(Abraham, R., Schneider, J. and Brocke, v, J., 2019)	Data governance specifies a cross-functional framework for managing data as a strategic enterprise asset. In doing so, data governance specifies decision rights and accountabilities for an organisation's decision-making about its data. Furthermore, data governance formalizes data policies, standards, and procedures and monitors compliance.
2	(Khatri, V. and Brown, C., 2010)	Data governance refers to who holds the decision rights and is held accountable for an organisation's decision-making about its data assets
3	(Otto, B., 2011)	Data governance refers to the entirety of decision rights and responsibilities regarding the management of data assets.
4	(Weber, K., Otto, B. and Osterle, H., 2009)	Data governance specifies the framework for decision rights and accountabilities to encourage desirable behaviour in the use of data. To promote desirable behaviour, data governance develops and implements corporate-wide data policies, guidelines, and

		standards that are consistent with the organisation's mission, strategy, values, norms, and culture
5	(DAMA., 2017)	DAMA (industry) – Data Governance is the exercise of authority and control (planning, monitoring, and enforcement) over the management of data assets.
6	(Thomas, G., 2020)	Data Governance Institute (industry) – Data Governance is a system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models which describe who can take what actions with what information, and when, under what circumstances, using what methods
7	(Benfeldt, O., 2017)	Data governance is companywide processes that specify decision-making rights and responsibilities aligned with organisational goals to encourage desirable behaviour in the treatment of data as an organisational asset
8	(Wende, K., 2007)	Data governance specifies the framework for decision rights and accountabilities to encourage desirable behaviour in the use of data (same as IT Governance)
9	(Kooper, M., Maes, R. and Lindgreen, R, E., 2011)	Information governance is a 'logical' alternative to IT governance, focusing on the seeking and finding, creation and use, and the exchange of information, and not solely on its production.
10	(Olaitan, O., Herselman, M. and Wayi, N., 2016)	a system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models which describe who can take what action with what information, and when, under what circumstances, using what methods
11	(Bruck, C., 2017)	Data Governance is the definition of methodological, conceptual, organisational, and technical rules, responsibilities, standards, and procedures aligned with the organisation's strategy and culture, with the goal of using data with their maximum potential within the organisational business processes
12	(Gartner., 2020)	Data governance is a framework of processes, policies, standards, and roles that ensures data is properly managed, secured, and used in line with the organisation's strategic objectives

Table 1. 3 Data/Information Governance Definitions

The definitions of data and information governance, while sharing some common themes, exhibit a wide range of interpretations and emphases. One recurring theme across many definitions is the emphasis on decision rights and accountabilities. For instance, Khatri and Brown (2010) define data governance as the assignment of decision rights and accountabilities over an organisation's data assets. Similarly, Otto (2011) highlights decision rights and responsibilities but extends the idea by including the management of data assets, emphasizing control over data as a core aspect. Thomas (2020) and the Data Governance Institute also focus on decision rights but add the concept of agreed-upon models that delineate specific actions and accountabilities related to data. Despite the similarity in focus, there are slight differences in the degree of formalization and the scope of accountability among these definitions.

Another major theme is the need for frameworks or structures to guide the governance of data. Weber et al. (2009) describe data governance as a framework for decision rights and accountabilities aimed at fostering desirable behaviours in data use. This view of governance as a means of behavioural control is shared by Wende (2007), who adds that the framework should also be consistent with an organisation's mission and values. Gartner (2020) also emphasizes the creation of processes, policies, and standards, but focuses more on the management and security of data in line with organisational objectives. In contrast, DAMA (2017) takes a more operational approach by defining data governance as the exercise of authority over data assets, including planning, monitoring, and enforcement, without necessarily emphasizing behavioural outcomes.

Despite these overlapping themes, significant differences in the scope and purpose of data governance emerge. For instance, Kooper et al. (2011) introduce a broader view by distinguishing information governance from IT governance. They argue that information governance should focus not only on the production of information but also on its exchange, use, and management within the organisation. This shifts the focus away from technical control and accountability, presenting a more holistic perspective on how organisations handle information. Bruck (2017) similarly broadens the scope by introducing the idea of technical, organisational, and methodological rules, linking data governance closely to organisational strategy and culture. This perspective adds an additional layer of complexity, implying that data governance is not just about decision rights or policies but also involves aligning data management practices with the overall business strategy.

What emerges from these varied definitions is the recognition that data governance serves multiple functions, ranging from controlling decision rights and responsibilities to fostering desirable behaviour and ensuring alignment with organisational strategy. However, the

differences in emphasis—whether on accountability, frameworks, or technical processes—highlight the lack of a universally agreed-upon definition for data governance. Each definition reflects the priorities and focus areas of different researchers and industry bodies, from DAMA’s focus on control and enforcement to Kooper et al.’s view of governance as part of the broader information life cycle.

This diversity of perspectives suggests that there is no single, commonly accepted definition of data governance. Instead, data governance is interpreted in ways that reflect the specific needs, contexts, and objectives of organisations. Some emphasize accountability and decision rights, while others focus on governance as a strategic tool for aligning data management with business goals. Others still adopt a more operational or technical lens, concentrating on the implementation of standards and policies. This lack of consensus implies that researchers and practitioners must carefully define the scope of data governance according to their research context, rather than rely on a one-size-fits-all definition.

This study will introduce a novel definition of data governance in Chapter 4 (Section 4.5) to address the detrimental impact of dark data within organisations. The proposed definition will capture the multifaceted nature and contextual factors of dark data governance as previously outlined. It will emphasize the pivotal role of holistic governance and its influence on an organisation's objectives and decision-making. Furthermore, the definition will provide strategic direction for the focus and scope of this research endeavour, aimed at mitigating the risks associated with dark data.

Section 1.3.2 examines the relationship between data governance and other governance frameworks, as well as the necessity of a holistic data governance approach to address the risks associated with dark data.

1.3.2 Data Governance and Other Governance Domains

This Section provides a more detailed discussion of the relationship between data governance and other governance domains. It examines how data governance relates to and complements broader organisational governance frameworks, such as corporate governance and information technology governance. The section explores how data governance must align with and support an organisation's overall strategic objectives and governance principles, while also highlighting the distinct focus and mechanisms of data-specific governance. Additionally, the section distinguishes data governance from data management, clarifying how governance provides the overarching decision-making and control structures to guide effective data management practices. Overall, this section offers a comprehensive view of data governance's place within

the larger landscape of organisational governance domains, highlighting the necessity of a holistic data governance approach to address the risks associated with dark data.

Governance is generally defined as the processes and structures by which an organisation sets, oversees, and achieves its strategic objectives ([Rau, G. K., 2004](#)). This notion has been expanded to encompass various governance domains, including corporate governance, data governance, information governance, and Information Technology governance. Consequently, it is crucial to examine the relationship between data governance and these other governance frameworks. Research on data governance can be traced back to the early 1980s, and it has since emerged as a prominent topic of interest for both industry and academic communities ([Hert, D. P. and Papakonstantinou, V., 2013](#)). Data governance practices should be aligned with and supportive of the broader corporate governance principles and strategic objectives of the organisation ([Wende, K., 2007](#)). Governance is broadly defined as the processes and decision-making structures that enable organisations to effectively manage and leverage their information technology resources in alignment with their overall strategic objectives. This concept should be distinguished from management, which focuses on the concrete implementation and execution of those governance decisions ([Khatri, V. and Brown, C., 2010](#)). Governance is crucial to facilitate effective data management. Data management encompasses the development, implementation, and supervision of plans, policies, programs, and practices to deliver, control, protect, and enhance the value of data and information assets throughout their lifecycles. Data governance, on the other hand, is defined as the exercise of authority and control over the management of data assets ([DAMA., 2017](#)).

Governance domains are emerging areas, and Researchers highlighted that it is easy to confuse between them. Therefore, it is critical for organisations to define context and alignment among governance domains ([Olaitan, O., Herselman, M. and Wayi, N., 2016](#)), ([Abraham, R., Schneider, J. and Brocke, v, J., 2019](#)), ([Bruin, D, R. and Solms, v, S., 2016](#)). The following provides further elaboration on key governance domains:

- **Corporate Governance:** Corporate governance refers to the frameworks and processes that establish the relationships and decision-making structures among a company's leadership, board, shareholders, and other key stakeholders. It provides the mechanisms through which the organisation's objectives are established and the means to achieve and monitor those objectives are determined ([Abu-Tapanjeh, M. A., 2009](#)). Weak corporate governance can result in mismanagement and corruption, whereas effective corporate governance promotes a fair and transparent business environment where organisations are accountable for their actions ([Dahlberg, T. and Nokkala, T., 2015](#)).

- **Internet Governance:** Internet governance encompasses the collaborative development and implementation of shared principles, norms, rules, decision-making processes, and initiatives by governments, the private sector, and civil society to guide the evolution and utilization of the internet ([Bauer, M. J., 2005](#)). Also, The term 'internet governance' was also used to refer to the management and regulation of the internet's underlying network infrastructure ([DeNardis, L., 2010](#)). While internet/web governance is not solely focused on infrastructure, the internet's content can be categorized into two main components: network infrastructure and data. Therefore, in terms of being recognized as a distinct governance domain, internet governance can be considered a subset that aligns with and complements other governance frameworks, such as IT governance, data governance, and cloud governance.
- **Information Technology (IT) Governance:** Information technology has become an integral and essential component for organisations, serving as the backbone that supports their operations and underpins their business activities ([Preittigun, A., Chantatub, W. and Vatanasakdakul, S., 2012](#)). Similar to corporate governance, IT governance can be defined as the process of establishing decision-making authority, assignment of responsibilities, and communication structures, along with the development of policies, standards, control mechanisms, and performance measurement systems. The purpose of these governance elements is to enable the fulfilment of defined organisational roles and responsibilities in the context of information technology management and alignment with overall strategic objectives ([Martínez, F. A. and Largo, L. F., 2009](#)). IT governance is defined as the processes and policies put in place to ensure that an organisation's information technology resources and systems support and align with its overall strategic objectives and goals ([Gheorghe, M., 2011](#)). Thus, Corporate governance can serve as a foundation for establishing IT governance frameworks and definitions ([Weber, K., Otto, B. and Osterle, H., 2009](#)).
- **Information Governance (IG):** Information governance can be characterized as the establishment of decision-making authority and an accountability framework to promote favourable conduct in the assessment, generation, storage, utilization, archiving, and deletion of information assets ([Silic, M. and Bäck, A., 2013](#)). The distinction between information governance and IT governance remains unclear for many organisations ([Davis, R. J., 2011](#)). Information governance can be viewed as a subset of corporate governance, with the main objectives being to improve the effectiveness of decisions and

processes within organisations, minimizing costs and risks, and maximizing the value derived from information assets ([Williams, P., 2007](#)).

- **Cloud Governance:** Cloud governance encompasses the establishment of policies that govern the factors of cloud service availability, security, privacy, location, compliance, and monitoring to ensure the enforcement of these policies when cloud-based applications are operational ([Woldu, L., 2013](#)). Cloud governance revolves around the relationships and interactions between cloud service providers and consumers, across various cloud business models and service delivery approaches ([Saidah, S. A. and Abdelbaki, N., 2014](#)). The business model should define the way in which an offer is made and how it is consumed. Cloud governance is part of the IT field and has not yet been given a clear definition. Cloud governance can be characterized as the establishment of policies that govern the factors of cloud service availability, security, privacy, location, compliance, and monitoring to ensure the enforcement of these policies when cloud-based applications are operational. The business model should define the framework for how cloud services are offered and consumed. However, cloud governance is part of IT and as a distinct domain has not yet been clearly defined in academic literature ([Woldu, L., 2013](#)).
- **Cybersecurity Governance:** Cybersecurity refers to the strategies, policies, and standards governing the security and operations within cyberspace. It encompasses a comprehensive range of activities, including threat reduction, vulnerability mitigation, deterrence, international cooperation, incident response, resilience, and recovery efforts. These policies and actions involve computer network operations, information assurance, law enforcement, diplomacy, military operations, and intelligence missions, all aimed at ensuring the security and stability of the global information and communications infrastructure ([NICCS., 2022](#)). ISO 27032:2012 demonstrates the close relationship between cybersecurity and information security, illustrating that they are not independent concepts. Rather, cybersecurity is appropriately situated within the broader domain of information security, as the security principles underpinning both are fundamentally the same, differing only in their specific implementation approaches.
- **Dark Data Governance:** The concept of 'dark data governance' has not been clearly defined or extensively explored within academic literature or industry practices.

The literature presents diverse perspectives on the relationships and interdependencies among the different governance domains, as illustrated in Figure 1.3, Figure 1.4, and Figure 1.5 below. There are varying views on what drives and influences the various governance frameworks and how they interact with one another.

According to the definitions and interrelationships of the various governance domains presented above, corporate governance serves as the highest-level governance domain, encapsulating all other governance types. It defines the decision-making frameworks and processes that ensure accountability, fairness, and transparency in an organisation's relationship with its stakeholders, including management, shareholders, and employees. It acts as the foundation upon which other governance frameworks, such as IT, information, and data governance, are built. This broad oversight role allows corporate governance to guide the alignment of all governance domains with the organisation's objectives, ensuring that resources are appropriately allocated, risks are mitigated, and ethical standards are upheld. IT governance emerges from corporate governance and focuses on ensuring that IT systems and resources are managed effectively to support the organisation's strategic objectives. IT governance deals with the alignment of IT and business strategy, the effective utilization of IT resources, risk management, and ensuring that IT supports organisational goals. It is closely related to both data governance and cloud governance, as these frameworks must align with IT governance policies and processes to ensure security, compliance, and performance. Data governance is frequently positioned as central to other governance frameworks. Figure 1.3 positions data governance at the core, emphasizing its foundational role in managing data as an asset. Data governance focuses on the decision rights, responsibilities, and frameworks for managing data throughout its lifecycle. This includes creating policies for data integrity, security, and privacy, which are critical for the organisation's overall decision-making processes. Figure 1.4 illustrates the interconnectedness between data governance, IT governance, and cloud governance, indicating that these governance frameworks must be implemented in a coordinated manner. Data governance ensures that data is accurate, secure, and compliant across cloud platforms and IT systems, while IT governance ensures the technology infrastructure supports these requirements. Cloud governance, which is still emerging as a distinct domain, ensures the policies governing cloud services align with broader data and IT governance principles, particularly regarding data storage, privacy, and security in cloud environments. Information governance extends beyond data governance, focusing on broader aspects of information management such as the creation, use, exchange, and archiving of information assets. While data governance deals with the granular control and oversight of data (structured and unstructured), information governance takes a more strategic view, ensuring that information flows effectively across the organisation, supports decision-making, and is used optimally in business processes. The most debated relationship among these governance domains has been between information governance and data governance, where researchers

and industry, for example, the Data Governance Institute, have consistently used information and data governance interchangeably, implying that the two domains mean the same thing. Another researcher debated that data governance is a prerequisite for information governance, and the argument stated that data governance must be part of both IT governance and corporate governance ([Olaitan, O., Herselman, M. and Wayi, N., 2016](#)).

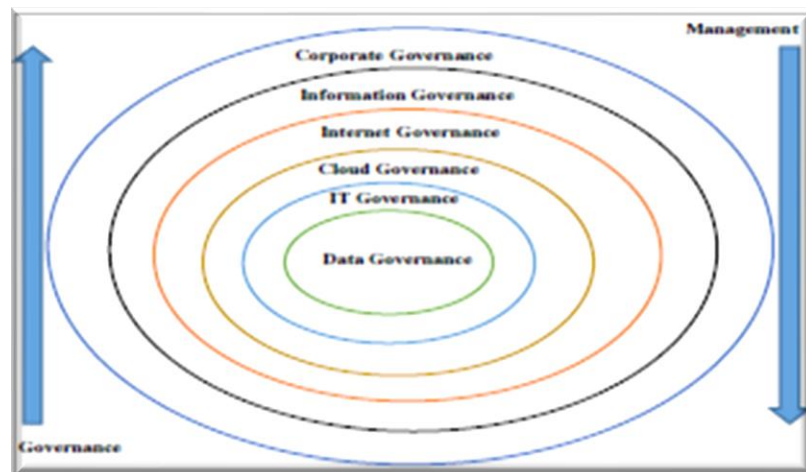


Figure 1. 3 Data Governance is at the centre of all other governance domains (Olaitan, O., Herselman, M. and Wayi, N., 2016)

Cloud governance, as illustrated in Figure 1.4, overlaps with both IT governance and data governance. This domain is focused on managing cloud resources—specifically, cloud service availability, security, privacy, and compliance. Cloud governance is vital as organisations increasingly move their data and applications to cloud platforms, creating a need for policies that govern the relationships between cloud service providers and consumers. These policies ensure that data governance standards (such as data privacy and security) are maintained even in cloud environments, while IT governance ensures that cloud platforms are used efficiently and in alignment with business goals. Cybersecurity governance is a key domain closely linked to data, IT, and information governance. It focuses on managing cybersecurity risks, ensuring the integrity and security of data, systems, and networks. The relationship between cybersecurity and information governance is especially important because information governance requires the secure management of information throughout its lifecycle. Cybersecurity governance ensures that data and systems are protected from breaches, attacks, and other cyber threats, creating a critical intersection with both IT and data governance domains.

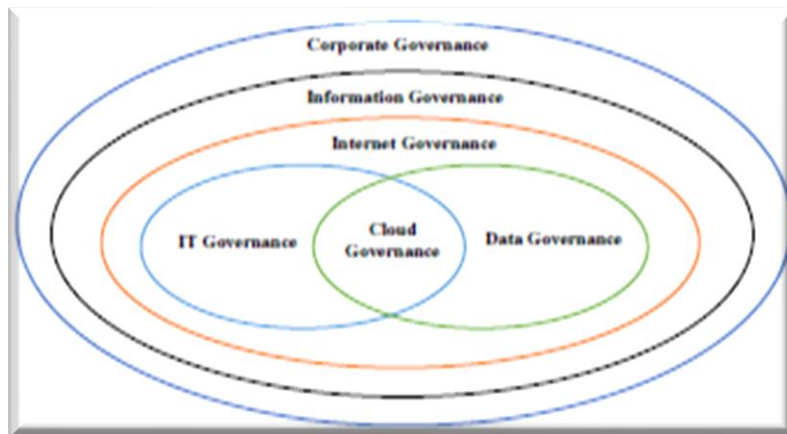


Figure 1. 4 Data Governance overlaps with IT Governance & Cloud Governance at the centre within the other governance domains (Al-Ruithe, M., 2018)

The various governance domains illustrated in the figures show how governance has evolved into a multi-layered structure where domains like corporate governance, IT governance, data governance, and cloud governance intersect. Corporate governance provides overarching guidance, while IT and data governance handle more specific functional areas (Figure 1.5). Information governance takes a broader, strategic approach to managing the flow and utility of information. However, there remains significant overlap and ambiguity, particularly between information governance and data governance.

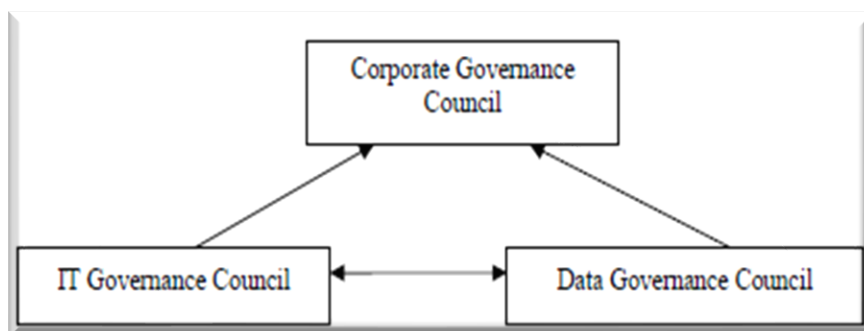


Figure 1. 5 Relationship between Corporate, IT, and Data Governance (Cheong, K, L. and Chang, V., 2007)

While some researchers and industry professionals use these terms interchangeably, others argue that data governance is a subset or prerequisite for information governance. This lack of clarity underscores the need for organisations to clearly define the boundaries and responsibilities within each governance domain to avoid confusion, ensure proper oversight, and optimize their use of data, information, and technology resources. Ultimately, while the governance domains are distinct, their effectiveness depends on how well they are aligned and

integrated. Organisations must ensure that these governance frameworks support one another, avoiding silos and fostering collaboration across corporate, IT, data, and cloud governance to meet organisational goals and manage risks comprehensively.

According to the analysis in this section, data governance currently lacks a common understanding or clear definition to guide both practitioners and researchers. This study proposes that data governance should be situated within the same contextual framework as other governance domains, as part of a novel, holistic governance model. Consequently, the governance of dark data should follow a similar contextual approach to that of other governance domains, enabling integration and alignment under a unified, holistic framework. Section 1.4 outlines the research problem statement and underscores the necessity of a holistic, integrated approach to governing dark data within an organisation's wider governance framework. Furthermore, the section elaborates on the underlying rationale and motivation for conducting this research.

1.4 Research Problem Statement and Motivation

Data governance focuses on the decision-making processes and the empowerment of people and procedures to enable an organisation to optimize the value it derives from its data assets ([DAMA., 2017](#)). While technological factors shape data management, the processes of governing technology and governing data are distinct. Organisations should refrain from allowing technology to dictate their data-related decisions; instead, they should let data requirements aligned with their overall business strategy guide their decisions about technology implementation ([DAMA., 2017](#)). Recent scholarly research has highlighted a transition towards a more encompassing data governance approach that leverages data governance as a strategic enabler to support an organisation's overall business objectives. This emerging paradigm motivates organisations to identify innovative opportunities that can enhance their competitive position in the market and generate a higher return on their data governance investments ([Curtiss, J., Saxena, S. and Seth, A., 2018](#)). However, the unfortunate fact is that bad data will always be with us no matter how much money organisations spend, and how much resources they employ in attempting to detect and prevent dark data ([Hand, J. D., 2020](#)), ([Veaux, D. D, R. and Hand, J. D., 2005](#)). As such, there is a crucial need for: first, to create awareness of the different types of dark data and their associated risks ([Hand, J. D., 2020](#)); and second, to govern dark data to ensure a desirable enhanced behaviour in the use of data to mitigate dark data risks while achieving organisational business goals ([Weber, K., Otto,](#)

[B. and Osterle, H., 2009](#)), [\(DAMA., 2017\)](#), [\(Khatri, V. and Brown, C., 2010\)](#), [\(Abraham, R., Schneider, J. and Brocke, v, J., 2019\)](#), [\(Otto, B., 2011\)](#), [\(Benfeldt, O., 2017\)](#), [\(Curtiss, J., Saxena, S. and Seth, A., 2018\)](#). Consequently, implementing effective dark data governance would necessitate a comprehensive transformation of the organisation's existing data governance approach, encompassing changes to its operating model, regulations, personnel, technology, and processes.

Given the risks associated with dark data, including security vulnerabilities, compliance breaches, and missed opportunities for value creation, a holistic approach to dark data governance is essential. Such an approach ensures that dark data is governed in alignment with broader organisational objectives, integrating all governance domains such as data governance, IT governance, information governance, and corporate governance. A holistic governance context helps address the complexity of dark data. Dark data often spans multiple sources and formats, residing in various systems, cloud services, or even within employee-created documents. Without a comprehensive governance strategy that involves multiple governance domains, organisations risk failing to identify or manage this data effectively. According to Weber et al. (2009), data governance must be tightly linked with IT governance to ensure that data policies are enforceable within the technological infrastructure. This is crucial for dark data, as much of it resides in IT systems that must be governed holistically to ensure secure and efficient data management. Moreover, corporate governance plays a key role in aligning dark data governance with an organisation's strategic objectives. Corporate governance frameworks guide decision-making and resource allocation at the highest levels of an organisation [\(Dahlberg, T. and Nokkala, T., 2015\)](#). Integrating dark data governance within this framework ensures that executive leadership is aware of the risks and opportunities posed by dark data. This awareness can lead to better-informed strategic decisions, such as investment in advanced data management technologies or the development of organisational policies that prioritize the management of dark data for business intelligence. A holistic approach also facilitates risk management by aligning dark data governance with cybersecurity governance and information governance. Unmanaged dark data can pose significant security risks, as outdated or forgotten data sets may not be protected with the latest security measures [\(NICCS., 2022\)](#). By incorporating cybersecurity principles into dark data governance, organisations can reduce the risk of breaches and ensure compliance with data protection regulations such as GDPR. Silic and Bäck (2013) highlight the importance of a holistic information governance approach to ensuring that data is managed, archived, and deleted in a way that minimizes risks. Without integrating cybersecurity and information governance principles, organisations may

overlook critical vulnerabilities within their dark data. Dark data governance requires a holistic context that aligns it with other governance domains, including data governance, IT governance, corporate governance, information governance, and cloud governance. This alignment enables organisations to manage dark data effectively, reduce risks, and extract value from previously untapped data sources. By integrating dark data governance into the broader organisational governance holistic context, organisations can ensure that dark data is not only controlled but also leveraged as a strategic asset, contributing to overall business objectives and enhancing organisational adaptability.

However, there is a scarcity of academic literature providing a comparable body of knowledge specifically focused on the governance of dark data. Researchers and practitioners have addressed the context and scope of data governance in various ways, without considering a comprehensive, holistic approach. One industry proposal advocated the use of dark analytics as a solution, where data was positioned as a strategic asset and competitive advantage by analysing and utilizing dark data in conjunction with an organisation's full data landscape, thereby bringing it into the light and capitalising on its strategic value ([Deloitte, P. U., 2017](#)), ([McNulty, K., 2017](#)). It has been noted that organisations may retain dark data solely for compliance reasons, as storing and securing such data often incurs greater costs and risks than the potential value it provides ([Deloitte, P. U., 2017](#)). Academics have proposed that organisations should be attentive to the potential risks associated with dark data. They have identified specific indicators that suggest invisible dark data may be distorting the collected data, as well as more general scenarios where potential dangers exist. To address these concerns, researchers have recommended a two-pronged approach. Firstly, they suggest creating a process to raise awareness about the various types of dark data, including the fifteen established types (Appendix-A) as well as any emerging ones. Secondly, they advise that organisations should recognize and understand the associated risks related to the different dark data types ([Hand, J. D., 2020](#)). Researchers have proposed other solutions for managing dark data, but these approaches have focused on partial or limited aspects rather than a comprehensive, holistic perspective. For instance, one study examined the infrastructure and policy dimensions involved in transitioning archived dark data to a high-performance computing environment, but did not consider the broader organisational context and governance requirements ([Purss, B. M. et al., 2015](#)). Another example focused solely on the organisational roles and responsibilities by proposing the introduction of a new position, the "Scientific Data Officer", to specifically address the management of dark data in addition to broader data handling duties ([Schembera, B. and Durán, M. J., 2020](#)). Another study proposed

a solution focused solely on developing a new data architecture by structuring previously unstructured data to address dark data challenges ([Karande, A. et al., 2019](#)). Additionally, one study outlined a dark data management model embedded within the information governance process, concentrating primarily on policies and procedures ([Ajis, M, F, A. and Baharin, H, S., 2019](#)). The existing solutions for addressing dark data risks exhibit sound approaches, but they have failed to propose a comprehensive dark data governance model that considers the holistic context at both intra-organisational and inter-organisational levels. Until recently, dark data governance has been largely informal, confined within specific data repositories, lacking structured processes and organisation-wide support ([Al-Ruithe, M., 2018](#)). Furthermore, organisations continue to face significant challenges in resolving issues related to data governance ([Hand, J, D., 2020](#)). The potential advantages of a holistic dark data governance across organisational boundaries are significant in enhancing the strategic value of data assets. Given these potential benefits, holistic dark data governance is a highly relevant research topic. The motivation for this research is the need to determine the context for an effective holistic dark data governance model, which will help organisations to maintain control of dark data risks while successfully achieving their business goals. Accordingly, this study undertakes a comprehensive examination of data governance and its contemporary role as a remedy for the growing challenges posed by dark data, as organisations strive to achieve their business objectives. Furthermore, the research explores how a holistic data governance model, and its associated control mechanisms, can guide organisations to sustain their goals while mitigating the various disturbances caused by dark data.

Therefore, the following key factors highlight the motivation of this study:

- Most of the current research on dark data governance focuses on partial or limited aspects of data governance, rather than taking a comprehensive, holistic approach.
- The existing research lacks a strong emphasis on the strategic value of dark data governance and how it can be integrated with an organisation's broader business goals and objectives.
- Current research on dark data tends to focus more on dark data management practices rather than the governance mechanisms required to effectively manage dark data. This results in a lack of consideration for the unique dimensions of data governance that arise from the need to integrate data governance and data management.
- The existing literature lacks a comprehensive conceptualization of a dark data governance model that considers an organisation's overall ability to adapt and the complexities of its operations (at intra- and inter-organisational levels within its environment).

- Researchers have not sufficiently explored the development of a holistic governance model that can accommodate various governance domains under a similar context, making integration across different areas easier to achieve.
- The existing literature lacks a comprehensive examination of organisations' need to mitigate risks associated with dark data. Dark data not only represents missed opportunities for valuable insights, but also poses potential financial and legal liabilities for organisations. It is necessary for corporate governance frameworks to be expanded to encompass data-related risks, ensuring that all data types are managed in alignment with the organisation's strategic objectives. Without a holistic governance model, organisations may be exposed to cybersecurity threats, data breaches, or regulatory penalties due to inadequate management of dark data.
- The lack of empirical studies that investigate dark data governance in a holistic context
- Organisations often lack the knowledge and guidance on how to design dark data governance models that are well-integrated within the broader organisational holistic context.

The underlying principle for this research arises from the concept that there is currently a lack of a holistic strategic approach to address the formalization of the dark data governance domain. This approach needs to be aligned with other relevant governance domains across the different organisational levels and within the context of the organisation's broader ecosystem. A holistic governance model that integrates dark data governance with the organisation's overall governance holistic context and strategic objectives is currently lacking in the existing research and practice. The motivation for this research lies in addressing the gaps in existing governance frameworks, reducing the risks associated with dark data, and enabling organisations to harness the untapped potential of dark data. By developing a holistic dark data governance framework, this research aims to contribute to the broader field of data governance and provide organisations with the tools necessary to manage their dark data effectively.

1.5 Aim and Objectives of the Study

The research aims serve as the main goals of the study, often encapsulating the broader purpose or intended outcomes. (Abdulai, T, R. and Owusu-Ansah, A., 2014). The objectives, on the other hand, are the specific and measurable steps taken to achieve the research aims. The alignment between the aims and objectives is crucial, as the methodology must be tailored to effectively address the research questions and fulfil the stated objectives.

The primary aim of this study is to conceptualize a novel, and holistic model of dark data governance that emphasizes cohesion and adaptability to mitigate the risks of dark data within organisational contexts. The proposed model is intended to serve as a diagnostic tool and a foundation for continuous improvements. Furthermore, this study aims to define a holistic dark data governance maturity model and its assessment framework to identify enhancements and facilitate continuous improvements in governing dark data, thereby supporting the achievement of organisational goals. To fulfil the research aims, the primary objectives of this study are:

- To explore potential dark data types that impact organisations in achieving their business goals - encountered during the execution of its business activities; in addition to understanding dark data risks and the need for holistic data governance to counteract dark data risks – Chapter 1
- To adopt a suitable methodology for this research - Chapter 2
- To conduct a comprehensive literature review (Chapter 3):
 - to understand the state of the art of data governance, including the organisational context, and existing frameworks for implementing dark data governance
 - identify challenges for implementing dark data governance
 - identify critical success factors as the key dimensions of holistic dark data governance
- To propose and conceptualize and develop a holistic dark data governance model (HDGM) within the context of “The Viable System Model - VSM” based on systems and cybernetics theories – Chapter 4
- To propose and conceptualize a holistic dark data governance viability maturity model (HDG-VMM) within VSM context – Chapter 5
- To propose and conceptualize a holistic dark data governance viability maturity assessment model (HDG-VMAM) to ensure continuous improvements within VSM context - Chapter 5
- To validate the proposed models and tools within the context of a leading university in the state of Texas, USA. To maintain anonymity, the selected institution is referred to as "University X" throughout the study – Chapter 6, and Chapter 7.
- To further evaluate the research outcomes, the study incorporated a practical assessment by examining the application of the assessment matrix across realistic case scenarios at three leading universities in Texas, USA. To maintain anonymity, the selected institutions are referred to as "University X", “University Y”, and "University Z” throughout the study.
- To draw conclusions and recommendations for future research directions to guide both practitioners and researchers – Chapter 8

1.6 Research Questions

In alignment with the outlined research aims and objectives, this study investigates the following research questions:

RQ1: What are the key components of dark data governance (both formal and informal) that organisations adopt to manage the power and impact of various types of dark data?

RQ2: How has the holistic data governance context affected the management of dark data? Holistic context: alignment of DG with other relevant governance domains (ex: IG, DM, IT Governance) across the locations of decision-making authorities (executive management, middle management, and operational level) within the different functions (ex: business, IT)

RQ3: Within the holistic data governance context, do the key DG concepts have similar emphasis within organisations in managing the different types of dark data?

1.7 Research empirical context and background - Leading Universities in Texas, USA)

In Texas, several universities have made substantial investments in data governance, though the specific application to dark data governance remains underdeveloped. The status of holistic dark data governance across universities in Texas, USA, reveals a mixed picture, where some institutions are progressing toward improved data governance, but there are still significant gaps, particularly concerning dark data management. Texas universities have established data governance structures aimed at comprehensively managing their institutional data assets, but the integration of dark data governance within these frameworks remains limited. Institutions like Texas A&M University and the University of Texas at Austin have established robust data and IT governance frameworks, but the need for a holistic approach to dark data governance is still emerging. For instance, Texas A&M University has formalized its IT governance framework, integrating various committees and leadership roles to improve alignment between IT services and institutional objectives (Texas A&M, 2018). Despite these advancements, the governance of dark data has not yet been fully integrated into these frameworks. Similarly, the University of Texas at Austin's data governance efforts are focused on improving data quality, transparency, and decision-making through initiatives like the Common Data Set, which enhances data accessibility for faculty and staff (UT@Austin, 2024). However, despite significant investments in infrastructure and analytics, specific strategies for addressing dark data remain unstructured.

The investments made in governance frameworks at Texas A&M and UT Austin have been supported by the University of Texas/Texas A&M Investment Management Company (UTIMCO), which manages over \$74.6 billion in endowment assets (UTIMCO, 2024). These funds support not only teaching and research but also initiatives related to data governance, although a focused strategy for dark data is still missing. The aim is to generate long-term investment returns to fund governance improvements. The need for dark data governance, however, remains a critical gap that both institutions must address to mitigate risks related to data security, compliance, and operational inefficiencies. Other universities, like the University of North Texas (UNT) and Texas Christian University (TCU), have robust data governance programs focusing on data accessibility, quality, and security, but dark data is often not specifically addressed as part of their frameworks (UNT, 2024), (TCU, 2021).

Texas universities have made significant progress in establishing robust data governance frameworks, yet the governance of dark data remains an underexplored area that requires a more comprehensive, integrated approach. The key challenges faced by these institutions include a lack of cohesion between various governance domains, such as data, IT, and cybersecurity, which are crucial for effectively managing dark data. Moreover, despite substantial investments, there is a limited emphasis on leveraging dark data to enhance decision-making and organisational efficiency. To address these challenges, universities should develop holistic dark data governance models that integrate continuous improvement processes across diverse governance domains. This would entail creating frameworks that align IT, data, and cybersecurity governance, and capitalising on the substantial financial resources available through endowment management to transform dark data into a strategic asset rather than merely managing it.

In light of the preceding discussion, this study evaluates the applicability and effectiveness of the proposed models and tools within the context of a prominent university in Texas, USA. To maintain anonymity, the institution is referred to as "University X" throughout the study. This university was selected due to its interest in data governance, accessibility to institutional data, and relevance to the researcher's geographic location. Residing in Texas enabled the researcher to engage with key stakeholders and gain first-hand insights into the institution's governance challenges and opportunities, facilitating data collection and empirical validation of the proposed models. The selection of University X as the research setting provided a valuable opportunity to assess the applicability and effectiveness of the proposed dark data governance models and tools within a real-world higher education environment. Leveraging the researcher's local knowledge and connections in Texas enabled a more detailed understanding

of the institution's unique data management landscape, which was crucial for validating the proposed models within the specific needs and constraints of the university. This on-the-ground approach ensured that the research outcomes were grounded in the practical realities faced by University X, enhancing the overall relevance and impact of the study. To further evaluate the research outcomes, the study incorporated a practical assessment by examining the application of the assessment matrix across realistic case scenarios at three leading universities in Texas, USA that were actively implementing general data governance practices but had not yet adopted a comprehensive approach to dark data governance. To maintain anonymity, the selected institutions are referred to as "University X", "University Y", and "University Z" throughout the study.

1.8 Research Contributions to Knowledge

This research project has made extensive and substantial contributions to knowledge. The study provides several important contributions to the field of data governance, with a particular emphasis on addressing the challenges associated with dark data within organisations. The key contributions of this research are summarized in Table 1.4.

Key Contribution	Summary of this Research Contribution to Knowledge
Identification of Research Gaps	Highlights significant gaps in current literature, particularly the lack of research on dark data as an organisational critical risk.
	Emphasizes the absence of holistic data governance frameworks addressing dark data within organisational and external contexts.
Advancing Knowledge	Evaluates the state of the art of data governance, with a focus on dark data governance.
	Identifies Critical Success Factors (CSFs) and challenges in implementing dark data governance frameworks in organisations.
Conceptualization of a Novel Holistic	Proposes a novel holistic dark data governance model within an organisational viable context.

Key Contribution	Summary of this Research Contribution to Knowledge
Dark Data Governance Model	Defines key systemic functions, communication channels, and information flows at both intra- and inter-organisational levels to counteract dark data.
	Validates the model in a real-world case scenario (University X) to ensure practical applicability.
Interdisciplinary Impact	Bridges gaps between disciplines, introduces cross-disciplinary approaches, and opens avenues for collaborative research.
	Unifies governance domains (corporate, IT, data governance) under a holistic context, simplifying their integration for the first time.
Development of a Novel Maturity Model	Introduces a novel holistic data governance maturity model as a foundation for continuous improvements.
	Validates the model in a real-world case scenario (University X) to ensure practical applicability.
Development of a Novel Maturity Assessment Model/Tool	Develops a maturity assessment tool to facilitate viability and maturity assessment of dark data governance.
	Validates the model in a real-world case scenario (University X) to ensure practical applicability.
Practical Application and Empirical Evaluation	Empirically validates research findings, models, and tools to verify their relevance and practical applicability in real-world organisational settings (in Universities X, Y, & Z).
Long-term Implications	Provides a foundation for future scholarly inquiries into dark data governance within a holistic organisational context.
	It has potential to drive transformative outcomes in holistic dark data governance over time.

Table 1. 4 The key contributions of this research to knowledge

1.9. Structure of the Thesis

The thesis is organised into eight chapters (see Figure 1.6), the content of which is summarized as follows:

- **Chapter One: Introduction to the Study**

This chapter outlines the purpose of the study, defining key concepts such as dark data and data governance, which form the foundation of the research. It introduces the nature of dark data and the role of data governance, followed by a discussion of the research problem and motivations behind the investigation. The chapter then presents the study's specific aim, key objectives, and research questions. Additionally, it highlights the potential contributions to academic knowledge and concludes by providing an overview of the thesis structure and organisation.

- **Chapter Two: Methodology**

This chapter outlines the methodology aligned with the aims and objectives of this study. The research is grounded in cybernetics and VSM frameworks, providing a holistic approach to data governance. The study employs a qualitative methodology, utilizing the Delphi method to gather expert consensus over three iterative rounds. This process involves structured questionnaires and feedback to refine and validate the proposed model, ensuring reliability and validity. Limitations of the Delphi method, such as potential bias and panel attrition, are addressed through careful planning, diverse expert selection, iterative design, and maintaining anonymity. The chapter also outlines measures taken to enhance the reliability and validity of the research findings.

- **Chapter Three: Tertiary/Systematic Literature Review of Dark Data Governance**

This chapter conducts a systematic review of the literature to assess the state of the art in data governance and dark data governance. It draws on previous works by accredited scholars and industry experts, examining critical success factors (CSFs) and barriers that influence the implementation of data governance and dark data governance practices. Through this review, the chapter provides a comprehensive understanding of the current landscape and key factors shaping effective governance strategies.

- **Chapter Four: A Strategic holistic Dark Data Governance model**

This chapter introduces a holistic model for sustaining dark data governance, grounded in the organisational Viable System Model (cybernetics and systems thinking). The model's conceptualization integrates findings from the systematic literature review and incorporates key Critical Success Factors (CSFs) to ensure its relevance and effectiveness in addressing the challenges of dark data governance.

- **Chapter Five: Dark Data Governance Maturity Model and Maturity Assessment Model**

This chapter introduces a maturity approach for dark data governance, designed to help organisations assess their current governance state and identify necessary improvements to align with organisational goals through continuous improvement. Additionally, a performance assessment matrix for evaluating dark data governance is presented.

- **Chapter Six: Validation of the Holistic Dark Data Governance Model**

This chapter discusses the validation process and results of the proposed holistic model designed to mitigate dark data risks and support organisational goals within a viable system context. The validation aims to verify the soundness and reliability of the research findings used in conceptualizing the model. A Delphi survey was conducted to validate the dark data governance model at University X, with a 60% consensus threshold applied to evaluate and assess the model based on the questionnaire findings.

- **Chapter Seven: Evaluation Validation of the Dark Data Governance Continuous Maturity Model and Maturity Assessment Model**

This chapter examines the validation of the proposed dark data governance maturity model and assessment matrix. The validation process aims to assess the rigor and reliability of the research findings used in developing both the maturity approach and performance assessment matrix. A Delphi study will be conducted to validate the proposed dark data governance maturity model and assessment matrix within University X. Furthermore, the dark data governance maturity instrument will be applied to evaluate the current state of dark data governance across three prominent universities in Texas, USA (X, Y, and Z), utilizing the maturity assessment matrix and generating a roadmap for improvements.

- **Chapter Eight: Research Conclusions and Recommendation**

This chapter summarizes the research outcomes and provides an overview of potential future directions for further exploration and development in the field.

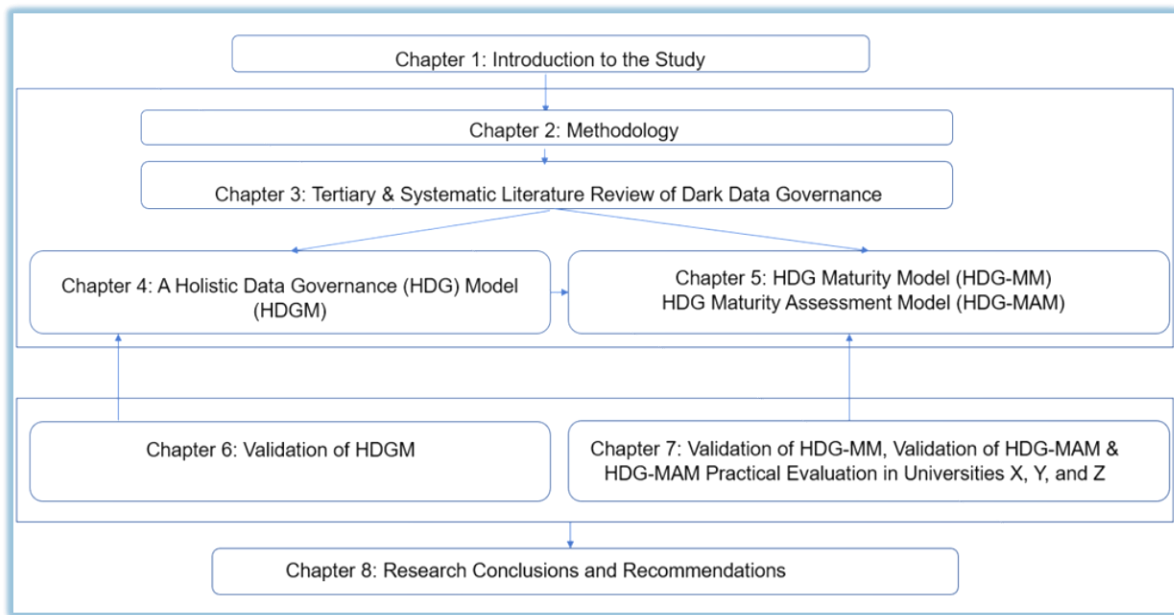


Figure 1. 6 Thesis Structure

Chapter 2. Methodology

2.1 Introduction

This chapter outlines the methodology aligned with the aims and objectives of this study. The research is grounded in cybernetics and VSM frameworks, providing a holistic approach to data governance. The study employs a qualitative methodology, utilizing the Delphi method to gather expert consensus over three iterative rounds. This process involves structured questionnaires and feedback to refine and validate the proposed model, ensuring reliability and validity. Limitations of the Delphi method are addressed through careful planning, diverse expert selection, iterative design, and maintaining anonymity. The chapter also outlines measures taken to enhance the reliability and validity of the research findings.

2.2 Aim and Objectives of the Study

The research aims of this study focus on conceptualizing a holistic dark data governance model that enhances cohesion and adaptability, allowing organisations to mitigate dark data risks and support continuous improvements. This model is intended as a diagnostic tool that facilitates the identification and mitigation of dark data risks while also aligning with organisational goals. To achieve this aim, the study's objectives include identifying the potential risks posed by dark data, conducting a comprehensive literature review on current data governance frameworks, and conceptualizing a model that considers intra- and inter-organisational factors. Additionally, the study seeks to develop a continuous improvement approach and an assessment framework to evaluate dark data governance maturity and foster ongoing enhancements (discussed in detail in Chapter 1 – Section 1.5).

2.3 Research Methodology

The research methodology is based on the concept of the research onion ([Zolfagharian, M. et al., 2019](#)) which defines Research questions, Paradigms, Theoretical frameworks, Research methods, Data collection and data sources, and Time horizon. These are illustrated in Figure 2.1 and described in the sub-sections below.

2.3.1. Research questions

In alignment with the research aims and objectives, this study investigates the research questions illustrated in Chapter 1 (Section 1.6).

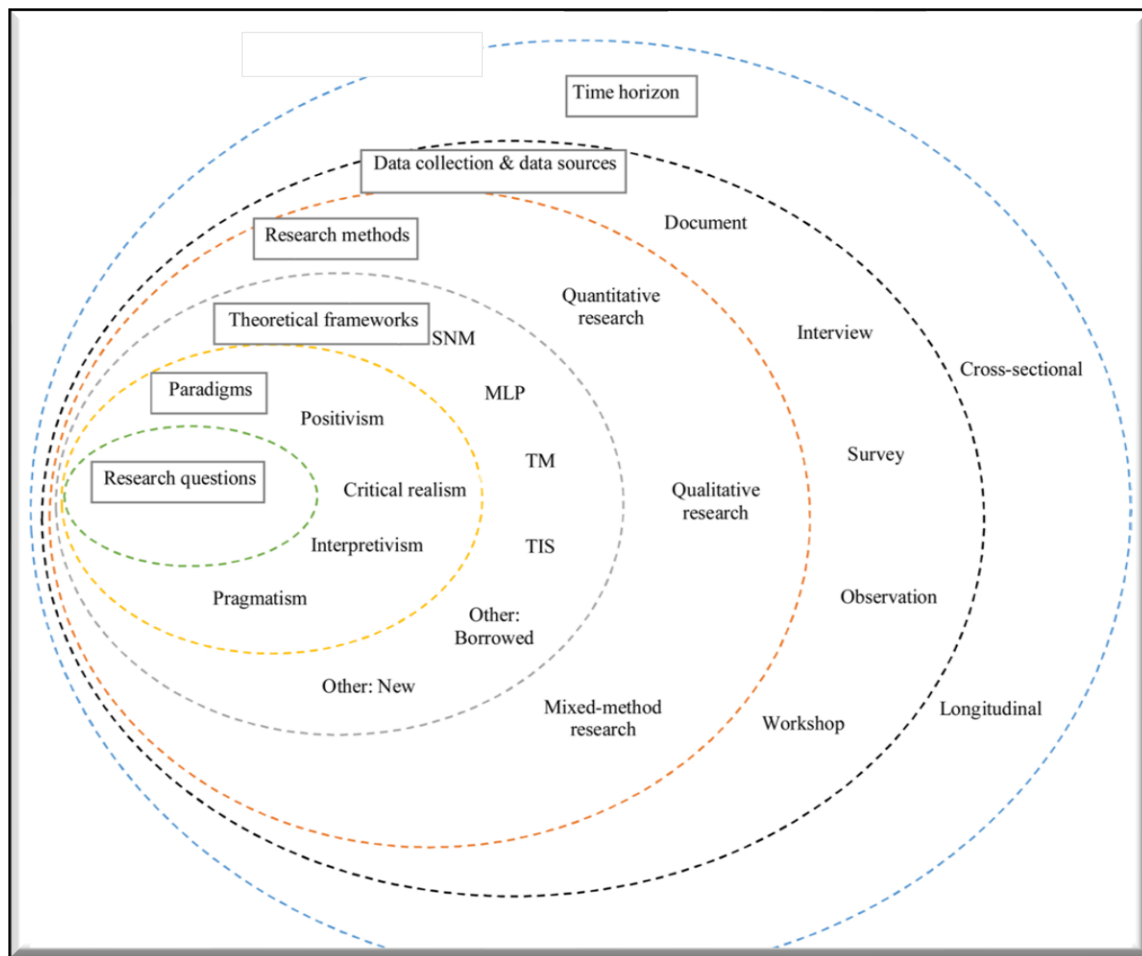


Figure 2. 1 The research onion ([Zolfagharian, M. et al., 2019](#))

2.3.2 Paradigms

The choice of an appropriate paradigm philosophy depends on the nature of the research domain and the available data sources. Positivism may be the suitable philosophical stance when the research primarily involves quantitative data that can serve as the basis for making predictions, such as in fields like demography or economic development. In contrast, if the research focuses on qualitative data, interpretivism or critical realism may be more appropriate philosophical perspectives. Interpretive positions are suitable when the research aims to construct narratives of the future and explore a range of future scenarios to provide insights. The critical realist perspective assumes that there are multiple possible futures which can be influenced to some degree from the present. This viewpoint is commonly used for scenario planning and analysis in areas such as social institutions, culture, and politics ([Melnikovas, A., 2018](#)).

This study adopts the Viable System Model (VSM) as its theoretical framework (see section 2.3.3). The VSM aligns with a 'functionalist' approach to systems thinking, which views

systems as objective components of reality that exist independently of the observer ([Reynolds, M. and Holwell, S., 2010](#)). This perspective considers systems as ontological entities that are part of the real world. However, an alternative 'interpretivist' perspective can also be applied when using the VSM ([Preece, G., Shaw, D. and Hayashi, H., 2013](#)). This interpretivist viewpoint recognises that multiple perceptions of reality coexist and may sometimes conflict. In this approach, systems are understood as epistemological constructs rather than ontological realities ([Reynolds, M. and Holwell, S., 2010](#)). When using the VSM to qualitatively describe, diagnose, or design data governance systems, an interpretivist paradigm is frequently adopted ([Zolfagharian, M. et al., 2019](#)). Consequently, this study will be guided by an interpretivist philosophical paradigm.

2.3.3 Theoretical Frameworks

Empirical investigations into data governance have improved our comprehension of the techniques employed to control data management. However, there has been limited research focused on developing a theoretical governance model capable of explaining and organizing the expanding range of governance components into a cohesive framework. To further advance the concept of data governance, the Viable System Model is proposed as a holistic theoretical framework for governance.

Since governance and cybernetics both deal with the control of sociotechnical systems, and Stafford Beer developed the Viable System Model as a framework for designing organisational control and communication ([Beer, S., 1972](#)), the VSM appears to be a suitable theoretical foundation for modelling IT governance ([Lewis, E., 2010](#)) and, by extension, data governance as well. The Viable System Model provides a robust theoretical foundation for developing a holistic model to govern the data governance function (further details are provided in Chapter 4). This is because the novel characteristics of the VSM enable the seamless integration of corporate governance, data governance, and IT governance at both intra-organisational and inter-organisational levels. This integrated approach allows an organisation to address the complexities arising from the convergence of past and future within a cohesive and adaptable context to achieve its goals.

2.3.4 Research methods vs. methodology

Methods refer to the specific techniques or procedures used to gather and analyse research data, while methodology encompasses the broader theoretical justification for the choice and

application of those methods ([Clough, P. and Nutbrown, C., 2002](#)). There is a common misperception that the terms "methodology" and "methods" are synonymous, as evidenced by the frequent practice of titling Ph.D. thesis chapters as "Methodology" when they primarily outline the data collection and analysis techniques employed ([Burton, L., 2002](#)).

This is not necessarily wrong; many such terms have conflicting and multiple meanings across the literature ([Crotty, M., 1998](#)), but in this research we will use a wider definition of methodology, referring to a theoretical justification for the methods used in a study ([Clough, P. and Nutbrown, C., 2002](#)), ([Burton, L., 2002](#)).

In an academic context, methods refer to the specific techniques and procedures employed to collect and analyse research data, while methodology encompasses the broader theoretical framework that justifies the choice and application of those methods ([Cousin, G., 2009](#)). The terms of the debate have been focusing on the distinction between three types of methodologies: quantitative, qualitative, and mixed (quantitative and qualitative) studies ([Borrego, M., Douglas, P. E. and Amelink, C., 2009](#)), ([Flick, U., 2010](#)). The choice of appropriate methodology is contingent upon the nature of the research questions being addressed ([Flick, U., 2010](#)). There is no single "correct" methodology or set of methodologies - the most suitable approach is determined by the specific research objectives. The methodological choices made in a research study are intertwined with the underlying theoretical perspective and epistemology. Methodology is positioned within four key components of the research process ([Crotty, M., 1998](#)):

- Methods: the specific techniques or procedures employed to collect and analyse research data.
- Methodology refers to the theoretical justification for the selection and application of specific research methods, aligning the choice and use of methods with the desired research outcomes.
- The theoretical perspective refers to the philosophical underpinnings that inform the chosen methodology, providing a contextual framework to support the logic and criteria of the research process.
- Epistemology refers to the theory of knowledge that underpins the chosen theoretical perspective and, in turn, informs the methodological approach adopted in the research study.

Accordingly, a quantitative methodology would not be suitable for this study, as qualitative research is often employed to address the limitations of quantitative approaches. The limitations inherent in quantitative research approaches are often used as a rationale for

employing qualitative research methodologies ([Flick, U., 2010](#)). Examining a qualitative research problem allows for the exploration of diverse perspectives, rather than a singular, definitive truth ([Brent, E. and Leedy, D. P., 2010](#)). Qualitative research examines specific cases within their temporal and spatial contexts, focusing on analysing people's behaviours and perspectives in their local environments ([Flick, U., 2010](#)). Qualitative inquiry is appropriate to research participants' lived experiences ([Caldas, M., 2009](#)). A quantitative research methodology is not appropriate for this study, as the goal is not to test hypotheses. Instead, the aim is to gather in-depth descriptions by eliciting participant responses through unstructured and structured narrative questions ([Janesick, J. V., 2011](#)).

Considering the aforementioned factors, this study will employ a qualitative methodological approach, which is well-suited to the exploratory nature of the research questions (Section 2.3.1) presented in Chapter 1 - Section 1.6. In order to address the different objectives to be achieved in this research, the findings of this research will be identified by a two-sequential phase approach. The steps to achieve these phases are listed as follows:

- Phase One: To conduct secondary research, which covered the following steps:
 - The study began with a comprehensive literature review to examine the current state of data governance and dark data governance. This review considered existing strategies and frameworks for implementing data governance, as well as the challenges and critical success factors that influence the implementation of dark data governance. Additionally, the results of a systematic review were evaluated and analysed to identify the key dimensions of data governance. This step helped to identify the research gap and is presented in Chapter Three.
 - The proposed Holistic Model: this model is based on the outcome of the systematic literature review, which includes the CSFs, existing frameworks and dark data governance key VSM systemic functions. The proposed model is formulated as a strategy to understand how to design, deploy and sustain an affective dark data governance system. This step is presented in Chapter Four.
 - Developing the dark data governance Maturity Model: this model aims to help organisations understand the current level of their dark data governance. More importantly, the maturity model can identify a path for the growth of dark data governance in the future. This phase is based on the results of the literature review, existing maturity models and the dark data governance model developed in Chapter Four. This step is presented in Chapter Five.

- Developing an assessment matrix to assess the dark data governance's level of maturity, in organisations. This assessment matrix aims to assess organisations and to enable continuous improvement process. This step will be based on the proposed model, the dark data governance maturity model and the existing assessment matrices in literature. This step is presented in Chapter Five.
- Phase Two: To validate and evaluate the research findings for the defined Delphi Study. This Phase covered the following steps:
 - Validating the proposed model through a Delphi study in University X (one of the top universities in Texas, USA). The validation will be conducted by a panel of experts from different departments in the university. This step is presented in Chapter Six.
 - Validating the proposed Maturity Model and its assessment matrix. The validation will be conducted by a panel of experts from different departments in the university. This step is presented in Chapter Seven.
 - Conducting a practical evaluation of the dark data governance assessment matrix for selected universities in Texas, USA. This step is presented in Chapter Seven.

2.3.5 Data collection and data sources

It has been argued that various research data collection methods may align well with certain methodological approaches and research contexts or questions, but there is not always a direct correspondence between data collection method and methodology. This is because researchers may employ the same data collection methods while holding quite distinct values and objectives in mind ([Cousin, G., 2009](#)). It has also been proposed that methods can be categorized into quantitative techniques, such as time series analysis, causal analysis, and trend analysis, as well as qualitative approaches, including Delphi surveys, futures wheel, and environmental scanning ([Melnikova, A., 2018](#)), ([Saleh, M. et al., 2008](#)). Given the complexity of our research problem and the appropriateness of the Delphi method for qualitative studies, this research will employ the Delphi methodology. The Delphi technique is a structured process for gathering information from subject matter experts in order to facilitate the formation of a reliable consensus, which can then inform effective decision-making. This approach involves a series of iterative questionnaires combined with controlled feedback, with the aim of synthesizing and consolidating data collected from individual experts and groups ([Keil, M., Lee, K. H. and Deng, T., 2013](#)). The Delphi technique is a structured methodology for gathering data from subject matter experts in order to enable the formation of reliable consensus that

can subsequently inform effective decision-making. This approach aims to prevent direct social interactions among participants that could potentially compromise the validity of the research findings ([Golkar, A. and Crawley, F. E., 2014](#)). The focus of Delphi method is on having participants in their natural setting and making sense of the results through an unbiased approach ([Venkatesh, V., Brown, A. S. and Bala, H., 2013](#)). For this study, the natural setting is the participants' work environments rather than focus group interviews or experimental conditions. The Delphi technique is an appropriate methodology for gathering and consolidating expert insights to forecast emerging trends and anticipated challenges related to the deployment, technical management, and core competencies required to effectively execute technical projects ([Janssen, J. et al., 2013](#)). The Delphi method is an appropriate approach for this study given the complex nature of the research problem and the need to gather and consolidate expert insights to effectively address the research questions and objectives. The data was gathered in three iterative rounds using a systematic approach to data collection and analysis. This process facilitated the refinement, development, and consensus-building of ideas among the expert participants (detailed in Chapter 6 and Chapter 7). The author designed the questionnaires based on the research objectives and questions. The Delphi study involved the administration of questionnaires over three separate rounds in validating the proposed models:

- Holistic Dark Data Governance Model (HDGM)
- Holistic Dark Data Governance Maturity Model (HDG-MM) and Holistic Dark Data Governance Maturity Assessment Model/Matrix (HDG-MAM)

Table 2.1, and Table 2.2 provide a concise overview of the data collection process, highlighting the key steps undertaken in the three rounds of data collection for the models (Further details in Chapter 6 – Section 6.3.2. and Chapter 7-Section 7.5).

Data Collection Round	Key Steps
Round 1*: Initial Validation of HDGM	*Awareness and training sessions were conducted as necessary
	Distributed Round-1 questions to validate the proposed model.
	Validated systemic design and key phases within the VSM context using closed questions with a five-point Likert scale.
	Collected participant suggestions via open-ended questions to refine the model.

Data Collection Round	Key Steps
	*Awareness and training sessions were conducted as necessary
Round 2*: Refinement and Further Validation of HDGM	Distributed Round 2 questions to build on Round 1 feedback.
	Validated systemic functions for key validated HDGM phases using closed questions with a five-point Likert scale.
	Collected further suggestions from participants through open-ended questions to enhance systemic functions
Round 3*: Final Validation of HDGM	Distributed Round 3 questions to finalise model validation and build on Rounds 2 validated feedback.
	Validated model usability within the VSM context using closed questions with a five-point Likert scale. Refined responses from Round 3 as necessary for final adjustments

Table 2. 1 Delphi three data collection rounds to validate HDGM

Data Collection Round	Key Steps
	*Awareness and training sessions were conducted as necessary
Round 1*: Validation of HDG-MM	Distributed Round-1 questions to validate the proposed HDG-MM.
	Evaluated the HDG-MM based on the selected assessment criteria using closed questions with a five-point Likert scale.
	Collected participant suggestions via open-ended questions to refine the model.
Round 2*: Initial Validation of HDG-MAM	Distributed Round 2 questions to build on Round 1 feedback and validate HDG-MAM.
	Evaluated the HDG-MAM based on the selected assessment criteria using closed questions with a five-point Likert scale.
	Collected further suggestions from participants through open-ended questions to enhance the model
Round 3*: Final	Distributed Round 3 questions to finalise HDG-MAM validation and build on Rounds 2 validated feedback.

Data Collection Round	Key Steps
	*Awareness and training sessions were conducted as necessary
Validation of HDG-MAM	Evaluated the model's individual constructs using closed questions with a five-point Likert scale.
	Collected further suggestions from participants through open-ended questions to enhance the model

Table 2. 2 Delphi three data collection rounds to validate HDG-MM and HDG-MAM

The author employed a combination of quantitative and qualitative data analysis techniques to validate the proposed models, leveraging the feedback provided by the participants. The participants represented a diverse range of roles, including senior leadership, specialized governance experts, and academia, with varied experiences in governance. The sample population selected for validation was appropriate for the scale of the study and included a balanced representation from University X. The participants held diverse positions, such as Data Governance Manager, IT Manager, President, Vice President, Director, Senior Analyst, Professor, Researcher, and Student. The participants were selected based on their homogeneity in education, in-depth knowledge, and extensive experience with data governance, Information Technology governance, and governance in general. This ensured a well-rounded and experienced group of experts, which enhanced the reliability and validity of the data. The data collection process aimed to gather feedback from various departments across different management levels simultaneously. To address potential inaccuracies in the participants' responses, the author provided them with background information to contextualize the study. This approach ensured a comprehensive understanding of perspectives and experiences, enhancing the reliability, validity, and depth of the feedback obtained. The quantitative feedback component involved the use of a five-point Likert scale to assess the validation criteria. Regarding the qualitative feedback, the validation process included open-ended statements, which allowed the participants to provide a rationale for their opinions and offer additional comments and recommendations to refine and enhance the model. It was essential to strike a balance between the validation results and the participants' suggestions to ensure the proposed models could be more effectively implemented across various institutions and organisations. The data analysis process involved a systematic approach to synthesizing

quantitative and qualitative feedback from the expert panel, with the goal of producing comprehensive and validated models that could be broadly adopted.

2.3.6 Time horizon

The time horizons typically considered in research studies can be classified into three main categories based on their duration: short-term (up to 10 years), medium-term (up to 25 years), and long-term (more than 25 years). These temporal scopes reflect the varying breadth and chronological frameworks within which research investigations are conducted ([Kosow, H. and Gassner, R., 2008](#)). Also, time was classified as a cross-sectional research design if it follows a relatively short time horizon or longitudinal research design if it is of long-term nature ([Zolfagharian, M. et al., 2019](#)). This component defines the temporal scope of the research - either a cross-sectional or short-term study, which involves data collection at a specific point in time, or a longitudinal design, which entails repeated data collection over an extended period to enable comparative analysis ([Melnikovas, A., 2018](#)).

For this study, a cross-sectional research design was deemed appropriate, as it aligns with the research's need for a short time horizon to address the research questions and collect data within a specific timeframe. The data for this study was collected during the first half of 2024, providing a focused and timely assessment of the research problem at hand.

2.4 Validity and Reliability

The Delphi method's structured and systematic approach facilitated the iterative refinement and enhancement of ideas, culminating in a more comprehensive and validated process to finalize the research outcomes. To ensure the reliability and validity of the analysis conducted using the Delphi technique, several measures were implemented:

- **Reliability:**

- **Consistency:** The Delphi study was conducted over three iterative rounds, allowing experts to review and refine their responses, ensuring consistency and stability in the data. Consistency in responses across rounds indicates reliability ([Hsu, C. and Sandford, A. B., 2007](#)).
- **Structured Questionnaires:** Structured and unambiguous questionnaires were used, tested for potential issues through awareness sessions and the data-gathering process. Ensured comprehensible questions for all participants ([Skulmoski, J. G., Hartman, T.](#)

[F. and Krahn, R. J., 2007](#)). experts were requested to identify issues and refine questions during the awareness sessions ([Hasson, F., Keeney, S. and McKenna, H., 2000](#)).

- Expert Selection: Experts were chosen based on stringent criteria, specifically their extensive experience and in-depth knowledge in the fields related to this study (e.g. data governance, IT governance, and overall governance practices) ensuring a reliable and highly informed panel. Establish clear criteria for selecting experts to ensure all participants have the requisite knowledge and experience, enhances data reliability ([Okoli, C. and Pawlowski, D, S., 2004](#)).

- **Validity:**

- Content Validity: The questionnaires were reviewed and refined through awareness sessions and the data-gathering process by the experts to ensure comprehensive coverage of the research topic. Ensure that questions cover all aspects of the research topic comprehensively. Collaborate with experts to refine the scope and avoid overlooking critical areas ([Hasson, F., Keeney, S. and McKenna, H., 2000](#)), ([Skulmoski, J, G., Hartman, T, F. and Krahn, R, J., 2007](#)).
- Construct Validity: Questions were grounded in relevant theories and literature, specifically Cybernetics and VSM theories, with consistency checks conducted through the three rounds of the Delphi study. Ensure questions are grounded in relevant theories and literature, establishing a clear link between the constructs being measured and the theoretical framework ([Okoli, C. and Pawlowski, D, S., 2004](#))
- Process Validity: A transparent and documented process was followed, detailing each step of the Delphi study ([J., E, J., Linstone, A, H. and Turoff, M., 2002](#)). Use iterative rounds not just for collecting data but also for refining and validating questions and responses ([Hsu, C. and Sandford, A, B., 2007](#)).
- Face Validity: Initial rounds focused on refining the questions with expert input to ensure they measured the intended constructs based on the research questions of this study ([Skulmoski, J, G., Hartman, T, F. and Krahn, R, J., 2007](#)).
- Consensus Measurement: The level of consensus among experts was assessed to confirm the model's systemic functions ([Hasson, F., Keeney, S. and McKenna, H., 2000](#)).
- Documentation and Reporting: Providing a detailed account of the Delphi process, including the selection of experts, rounds of questioning, methods of analysis, and how consensus was reached ([Okoli, C. and Pawlowski, D, S., 2004](#)).

- Transparency: Be transparent about any limitations (addressed in section 2.5) encountered during the process and how they were addressed ([Hasson, F., Keeney, S. and McKenna, H., 2000](#)).

The implementation of these methodological measures was intended to ensure the Delphi technique employed in this study generated reliable and valid data, thereby strengthening the robustness of the research findings. This approach was designed to enhance the credibility of the outcomes, enabling the effective refinement of the proposed model of dark data governance, including its maturity model and assessment matrix.

2.5 Limitations

Researchers should thoroughly acknowledge the limitations inherent in their studies. Identifying and addressing the constraints and shortcomings of a research design is a crucial component of academic integrity ([Roberts, M, C., 2010](#)). Limitations are specific aspects of the study design that are known to potentially undermine or compromise the validity of the results ([Roberts, M, C., 2010](#)). This Delphi study enables the data collection from the panel of experts completing questionnaires for all three rounds ([Brady, R, S., 2015](#)), ([Yousuf, I, M., 2007](#)). The following provides the key areas of limitations in relation to a Delphi study research design.

- To ensure the expert panel is relative and credible to completing the governed procedures necessary for a Delphi study, the selected experts must meet the required selection criteria instead of personal preference ([Adler, M. and Ziglio, E., 1996](#)). The selection of experts can introduce bias if not carefully managed. The credibility of the Delphi study largely depends on the expertise and diversity of the selected panelists ([Hsu, C. and Sandford, A, B., 2007](#)).
- The lack of interaction among the panel of experts may allow other panel members to question if their ideas were fully understood thus creating an adverse impact on effective communication due to lack of verbal clarification ([Delbecq, L, A., Ven, d, V, H, A. and Gustafson, H, D., 1976](#)).
- The wording of the questionnaire may lead to a bias response. The panel of experts may provide answers they believe the researcher wants instead of replying with their true thoughts and ideas in relation to the study's questionnaire ([J., E, J., Linstone, A, H. and Turoff, M., 1976](#)).

- The specificity to the amount of the experts' experience could lead to low quality of responses while simultaneously impacting the credibility of results or a wider audience base ([Bijl, R., 1992](#)).
- The iterative nature of the Delphi method, requiring multiple rounds of questionnaires and feedback, can be time-consuming participants. This may lead to participant fatigue and drop-out, potentially affecting the study's results ([Okoli, C. and Pawlowski, D, S., 2004](#))
- Maintaining anonymity in Delphi studies can be challenging ([Keeney, S., Hasson, F. and McKenna, H., 2001](#))

Effectively addressing the limitations inherent in Delphi studies necessitates careful planning and implementation across various aspects of the research design and process. This study employed the following strategies to mitigate these limitations:

- Selecting the Panel ([Hsu, C. and Sanford, A, B., 2007](#)): Experts with diverse backgrounds were carefully selected
- Mitigating Limited Depth of Insight ([Skulmoski, J, G., Hartman, T, F. and Krahm, R, J., 2007](#)): This study used a mixed-methods approach that incorporates both quantitative measures and qualitative data collection, such as open-ended questions, to gain a richer, more nuanced understanding of expert opinions
- Addressing Design Rigidity ([Hsu, C. and Sanford, A, B., 2007](#)): this study followed iterative Design to allow for flexibility in the questionnaire design by revising and refining questions based on feedback from initial rounds. This iterative approach helps capture emerging themes and unexpected insights.
- Reducing Response Bias ([Rowe, G. and Wright, G., 1999](#)): This study ensured the anonymity of responses to reduce social desirability bias and encourage honest and uninfluenced input from participants .
- Enhancing Consensus Measurement ([Keeney, S., Hasson, F. and McKenna, H., 2001](#)): This study used a variety of statistical measures to better capture the level of consensus.
- Preventing Panel Attrition ([Okoli, C. and Pawlowski, D, S., 2004](#)): The author ensured the process is not overly lengthy or burdensome and kept the participants engaged by communicating the importance of their contributions for completing all rounds.
- Interpreting Statistical Results ([Mullen, P., 2003](#)) : This study provided clear explanations and context for statistical findings by using visual aids such as graphs and charts to make the data more accessible and understandable

- **Balancing Quantification with Qualitative Insights** ([Yousuf, I. M., 2007](#)): This study followed a holistic analysis approach by balancing the emphasis on quantitative data with qualitative insights to ensure a comprehensive understanding of the research problem. Highlight how qualitative feedback informs and complements quantitative results.
- **Addressing Complex Issues** ([Hasson, F., Keeney, S. and McKenna, H., 2000](#)): This study followed adaptive questioning by design questions that are capable of capturing the complexity of the issue being studied. Allow for adaptive questioning that can evolve based on responses from previous rounds.
- **Ensuring Content Validity** ([Keeney, S., Hasson, F. and McKenna, H., 2001](#)): This study ensured that the questionnaires were reviewed by the experts during the awareness sessions to ensure they covered all relevant aspects of the topic comprehensively before distributing them.
- **Enhancing Process Validity** ([Hsu, C. and Sandford, A. B., 2007](#)): This study maintained a transparent and well-documented process for all rounds of the Delphi study, detailing each step and the rationale behind it to enhance credibility and replicability.

By implementing these strategies, researchers can mitigate the limitations of Delphi studies, whether qualitative or quantitative, and enhance the reliability, validity, and overall robustness of their research findings.

2.6 Ethical Considerations

Ethical considerations were a crucial component of the research design ([Fox, J., Murray, C. and Warm, A., 2003](#)). The study adhered to institutional ethical protocols, with the research plan approved by the university's ethics committee (Appendix B). Participants were informed about the study's purpose and assured of anonymity in their survey responses. A consent form was provided to confirm participants' voluntary involvement, with the option to withdraw at any time. Contact details for the researcher, supervisor, and the university's ethics committee were provided, allowing participants to raise any ethical concerns. Crucially, participants were provided with assurances that their data would be treated confidentially and anonymously and that any published findings would not enable individual identification. These ethical safeguards were implemented to protect the rights and well-being of the study's participants, ensuring the research was conducted in an ethical and responsible manner.

2.7 Chapter Summary

This chapter outlines the methodology aligned with the aim and objectives of this study focusing on developing and validating a Holistic Dark Data Governance Model based on cybernetics and Viable System Model theories. The primary goal is to create a novel model for managing dark data, ensuring cohesion and adaptability within an organisational context. Key objectives involve identifying dark data risks, conducting a comprehensive literature review, developing the HDGM, and proposing a continuous improvement and maturity assessment approach for dark data governance. The research is grounded in cybernetics and VSM frameworks, providing a holistic approach to data governance.

The study employs a qualitative methodology, utilizing the Delphi method to gather expert consensus over three iterative rounds. This process involves structured questionnaires and feedback to refine and validate the proposed model, ensuring reliability and validity. Limitations of the Delphi method, such as potential bias and panel attrition, are addressed through careful planning, diverse expert selection, iterative design, and maintaining anonymity. The chapter also outlines measures taken to enhance the reliability and validity of the research findings.

Chapter 3. Tertiary Literature Review of Data Governance and Dark Data Governance

3.1. Introduction

Data governance has emerged as a critical management discipline in recent years, driven by the growing importance of data assets and the need to effectively manage them ([Gregory, A., 2011](#)). Organisations, including higher education institutions, are increasingly recognizing the significance of data governance in aligning their information technology efforts with business processes and achieving their organisational goals ([Jim, K. C. and Chang, H., 2018](#)). The concept of data governance encompasses the policies, procedures, and accountabilities established to ensure the effective management and utilization of an organisation's data resources ([Gregory, A., 2011](#)). Data Governance provides a framework for developing a data governance program in a higher education setting, highlighting the crucial role that institutional research offices can play in building institutional capacity for a well-documented and managed data landscape ([Hubbard, D., Freda, A. and Swanagan, A., 2020](#)). Furthermore, Data governance emphasizes the strong links between corporate governance, risk, and compliance, and how data underpin all three, necessitating effective data governance to maximize the value of data assets and mitigate organisational risks ([Gregory, A., 2011](#)). Recent developments in big data have heightened the need for data governance across various sectors, including higher education ([Jim, K. C. and Chang, H., 2018](#)). While multiple research efforts focus on a literature-based approach to conceptualizing data governance, evidence-based research on this topic is scarce ([Jim, K. C. and Chang, H., 2018](#)) especially holistic data governance. In the rapidly evolving digital landscape, the importance of effective data governance has become crucial. With the surge of big data and the increasing complexity of data and information management, organisations must adopt a holistic approach to ensure the value, security, and compliance of their data assets ([Smallwood, F. R., 2012](#)). The foundation of holistic data governance lies in recognizing data as a strategic organisational asset that transcends traditional IT boundaries ([Al-Ruithe, M., Benkhelifa, E. and Hameed, K., 2018](#)). This shift in perspective necessitates the alignment of data management practices with broader corporate governance structures, policies, and decision-making processes. At the core of holistic data governance is the establishment of clear roles, responsibilities, and decision-making frameworks. ([Abraham, R., Schneider, J. and Brocke, v. J., 2019](#)). Effective data governance necessitates the integration of diverse stakeholders and subject matter experts, cultivating a shared mindset across the enterprise where quality data is not merely achieved, but actively valued and leveraged to drive

organisational goals. By cultivating a collaborative culture, organisations can establish a shared comprehension of data assets, their related risks and prospects, and the suitable controls to ensure they support the achievement of organisational objectives. The domain of data governance has expanded beyond its initial emphasis on data quality and regulatory compliance to encompass a more comprehensive set of considerations. These include data privacy, information security, and the effective utilization of data to inform strategic decision-making. This broader scope necessitates a comprehensive approach that aligns data governance with an organisation's broader objectives and risk management strategies. Ultimately, holistic data governance is not just about the technical aspects of data management, but the ability to cultivate a data-driven culture that values information as a strategic asset. Integrating data governance into the organisation enables leaders to unlock the full potential of their data, fostering innovation, operational efficiency, and regulatory compliance to achieve organisational goals.

This chapter aims to offer a thorough examination of the current state of data governance and its expansion into the domain of "dark data," emphasizing the key challenges and the critical factors for success within this evolving field. The tertiary review in this chapter considers previously published research on data governance conducted by academic researchers and industry practitioners. The main objective is to assess the current state of knowledge regarding data governance, including its application to the domain of dark data governance, and to identify potential research directions based on the existing literature. This study undertakes a comprehensive tertiary review to identify the requirements, existing frameworks, key challenges, and critical success factors for implementing dark data governance, drawing insights from previous research publications. Accordingly, this study conducts a detailed examination of data governance and its role in organisations and institutions, with a particular emphasis on dark data governance within a holistic organisational context.

3.2. Review Process Description

This section outlines the methodology adopted to conduct a comprehensive and rigorous literature review. The purpose of the literature review is to systematically gather and critically analyse all relevant research pertaining to the study's objectives, with the aim of generating objective and unbiased findings. The literature review objectives are the driving force behind the methodology, which is a crucial step in this process. In this study, the research objectives focus on identifying and examining the existing frameworks, initiatives, and proposals related to data governance that have been designed for implementation in data management domains

broadly, as well as specific to the realm of dark data management. This chapter aimed to fulfil the objectives outlined in the literature review questions presented in Table 3.1. These questions guided the determination of the content and structure of the literature review, as well as the selection, critical evaluation, and analysis of the primary studies. This study adopted the tertiary review structure, as described by key authors ([Kitchenham, B. and Charters, S., 2007](#)), ([Cruzes, S. D. and Dybå, T., 2011](#)), ([Budgen, D. et al., 2018](#)), ([Hummel, M., 2014](#)), ([Guides, L. U., 2023](#)), and ([Mulrow, C. and Cook, D., 1998](#)) to identify, evaluate, and synthesize all available research sources relevant to our research questions. Tertiary study is a systematic review of systematic reviews and uses the same methodology as a standard systematic literature review. A tertiary review is a comprehensive examination of existing systematic reviews, employing the same rigorous methodological approach as a standard systematic literature review. It aims to consolidate and synthesize the findings from multiple secondary sources to provide a thorough understanding of the research topic ([Kitchenham, B. and Charters, S., 2007](#)). A Tertiary study uses also, primary sources and consolidates both primary and secondary into one source. Tertiary-level publications can serve as useful starting points for research initiatives, as they typically synthesize and condense the key themes or key insights distilled from extensive bodies of literature into a concise, accessible format ([Guides, L. U., 2021](#)). The primary motivation for conducting a tertiary review is to systematically categorize and synthesize the existing body of knowledge on data governance and dark data governance. By comprehensively identifying and evaluating relevant research publications, this approach aims to provide a thorough and unbiased understanding of the current state of dark data governance research and practice. Classifying the existing publications facilitates researchers in obtaining a comprehensive understanding of the current state of data governance research as well as the prevailing gaps in dark data governance research. Concerning the tertiary literature review approach, numerous studies in the literature have employed this methodology to investigate the state-of-the-art of various subject areas ([Cruzes, S. D. and Dybå, T., 2011](#)), ([Cadavid, H., Andrikopoulos, V. and Avgeriou, P., 2020](#)), ([Imtiaz, S. et al., 2013](#)), ([Verner, J. et al., 2014](#)). The goal of the study in ([Cruzes, S. D. and Dybå, T., 2011](#)) as a tertiary review is to investigate the types and approaches of research synthesis employed in systematic reviews within the software engineering domain, with the aim of enhancing the understanding of the key challenges and the implications for advancing relevant research and practice. The tertiary review in ([Cadavid, H., Andrikopoulos, V. and Avgeriou, P., 2020](#)) seeks to investigate the current state of research on System of Systems (SoS) architecting in order to enhance the broader community's understanding of the SoS concept. The study ([Imtiaz, S. et al., 2013](#)) aims

to document the reported experiences of researchers conducting Systematic Literature Reviews in software engineering. This is intended to benefit new researchers who wish to undertake Systematic Literature Reviews for the first time. The tertiary study ([Verner, J. et al., 2014](#)) examines systematic literature reviews on global software development research to assess whether they provide suitable guidance on risks and risk mitigation strategies for organisations engaged in global software development. The study included scientific and industry sources that focused on data governance. The selected articles had to be full-text, peer-reviewed publications on data governance and dark data management, published in English between 1995 and 2023. Exclusion criteria were also applied (see Table 3.2).

3.3. Tertiary Literature Review Questions

Formulating the review questions is a crucial step in a literature review (Kitchenham, B. and Charters, S., 2007). This study seeks to explore two principal research questions through the literature review process. The specific research questions are outlined in Table 3.1.

Research Questions (RQs)	Motivation
What is the state of the art of research on data governance to mitigate dark data?	The aim is to find out which aspects of data governance in the dark data have been researched and which have not been researched. This review helps this study to identify what solutions are offered for data governance at large and dark data in specific. Also, the aim is to understand the existing gaps in the data governance frameworks and process in dark data management.
What is the state of the art of research on data governance at large?	The aim is to find out what aspects of data governance at large have been researched, and to identify the gaps in this area to support the main aim of this study.

Table 3. 1 Review Questions and Motivation.

3.4. Inclusion and Exclusion Criteria

In conducting a tertiary review, the researcher must clearly define the search parameters to ensure a focused and high-quality review. This involves establishing well-defined inclusion

and exclusion criteria, as outlined in the works of key authors ([Hummel, M., 2014](#)) ([Guides, L. U., 2021](#)), and ([Mulrow, C. and Cook, D., 1998](#)). As detailed in Table 3.2, the inclusion and exclusion criteria were applied to the search protocol. The primary aim of the study selection process was to identify publications that provide relevant evidence pertaining to the research questions ([Kitchenham, B. and Charters, S., 2007](#)), ([Guides, L. U., 2021](#)). This tertiary literature review consolidates and organises the selected sources into a coherent format, extracting the key findings and synthesizing the most key aspects from the extensive body of literature. The resulting synthesis serves as a well-positioned starting point for future research initiatives. The inclusion and exclusion criteria were established to guide the literature search. The search terms used included 'data governance', 'information governance', 'dark data governance', as well as related terms such as "data governance organisation", "governance data", "dark data", "bad data", "dirty data", "information governance", "IT governance", "data quality", "information quality", and "data management". These search terms were combined using the Boolean 'OR' operator to capture a comprehensive set of relevant publications.

Inclusion criteria	Exclusion criteria
Directly related to data governance, dark data governance, information governance, data quality governance	Irrelevant to study of data governance or dark data governance or information governance or data quality governance
Data governance frameworks design	Not peer-reviewed papers
Data and dark data governance solutions applied in organisations	Duplication Publication
Data and dark governance challenges	Journals not accessible online
Peer-reviewed	Industry professional papers
Written in English	Not written in English

Table 3. 2 Inclusion and exclusion criteria for the tertiary review

3.5. Defining the Review Protocol

This literature review adopts a concept-centric approach, organizing and presenting the publications according to the specific areas of data governance that they address. The research protocol is a crucial methodological component, as it adds rigor and value to the research

objectives and goals. This section aims to define the review protocol used to systematically examine the existing literature on data governance in general and dark data governance in particular. The steps followed in conducting this review were informed by the work of Kitchenham and Charters ([Kitchenham, B. and Charters, S., 2007](#)) and of other key researchers ([Cruzes, S. D. and Dybå, T., 2011](#)), ([Mulrow, C. and Cook, D., 1998](#)), as illustrated in Figure 3.1.

The review protocol comprises four key steps:

- **Step 1:** An academic exploration of scientific and practice-oriented literature was conducted, focusing on data governance and related concepts. The search included terms such as "data governance," "data governance organisation," "govern data," "data governance in other domains,"; dark data, bad data, dirty data, and "dark data governance." The search protocol was applied across various reputable academic online databases (see Table 3.3). In addition to academic sources, the search also considered practice-oriented literature, including papers and reports published by industry associations, software vendors, and leading companies and consultancies (Figure 3.2). The search focused on the article title, abstract, keywords, and publications between 1995 and 2023 for both data governance and dark data governance.
- **Step 2:** The sources were analysed by categorizing them into two types based on the nature of their contribution: scientific and practice-oriented. The scientific format encompasses academic publications such as journal articles, conference papers, books, working reports, and theses. The practice-oriented format includes publications by industry associations, software vendors, and leading companies or consulting firms (see Table 3.4). This step entails categorizing the sources based on key parameters, such as the nature of their contribution (whether scientific or practice-oriented), the format type (e.g., journal article, industry report), and the source's reference.
- **Step 3:** This step employs critical literature review techniques to thoroughly examine the current state of research on data governance and dark data governance, which supports the research objectives. Additionally, the author compared the work of various authors in the data governance domain to identify any contradictions or inconsistencies within the existing body of knowledge. This analytical approach contributes to the research by pinpointing gaps that do not appear to have been addressed by prior studies.
- **Step 4:** The author identified the research gap and explained how to fill this gap.

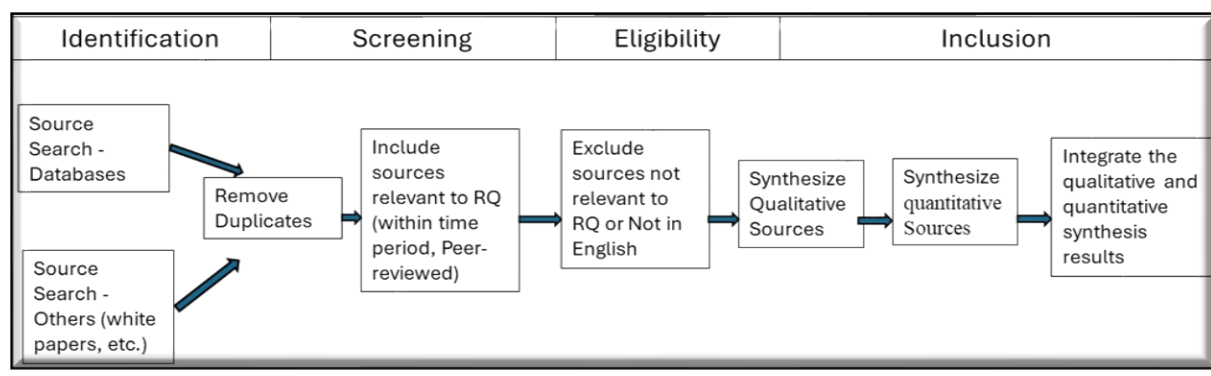


Figure 3. 1 The main process used to conduct the tertiary literature review

No.	Name
1	ScienceDirect
2	SpringerLink
3	IEEE Xplore
4	Google Scholar
5	JSTOR
6	ProQuest
7	ACM Digital Library
8	EBSCOhost Databases
9	CiteSeerX
10	SAGE
11	ResearchGate
12	ICSCAN Proceedings
13	Google

Table 3. 3 Database of sources used for searching academic literature

3.6. Search Results and Study Selection

By applying the search protocol and study selection process outlined in Section 3.5, the primary studies were identified. As illustrated in Figure 3.2, the primary study selection for data governance was conducted in four stages. In the first stage, 3,700 sources were identified from various databases and sources. The second stage involved analysing the titles of these 3,700 sources, which resulted in the selection of 230 articles that appeared to be relevant to the systematic research topic. In the following stage, the abstracts and keywords of these 230 articles were reviewed, which led to the identification of a total of 113 articles that met the inclusion criteria. Finally, at the last stage, duplicate papers were removed, yielding 82 unique papers for the final in-depth review and analysis.

The study selection process involved collecting and analysing various metadata from each article, including the publication format (e.g., journal article, conference paper, industry report), source name (e.g., academic journal, industry publication), publication date, author

information, article title, and the nature of the source's contribution (whether it was from an academic or practice-oriented perspective). This comprehensive data collection and categorization process allowed for a deeper understanding of the landscape of research and industry publications on data governance and dark data governance (Table 3.4 and Table 3.5). Table 3.5 presents the main findings of each Source. Table 3.4 Detailed Categorization of 82 Records on Data Governance and Dark Data Governance from the Defined Search Protocol. The records were categorized into four groups based on their academic or practice-oriented nature, as well as their focus on either data governance or dark data governance:

- Academic DG: A collection of academic publications, such as journal articles, conference papers, and theses, that address data governance.
- Academic Dark DG: Academic publications focused on the topic of dark data governance.
- Practice-Oriented DG: Practice-oriented literature, including industry reports, white papers, and publications from companies and consultancies, on data governance.
- Practice-Oriented Dark DG: Practice-oriented sources addressing the topic of dark data governance

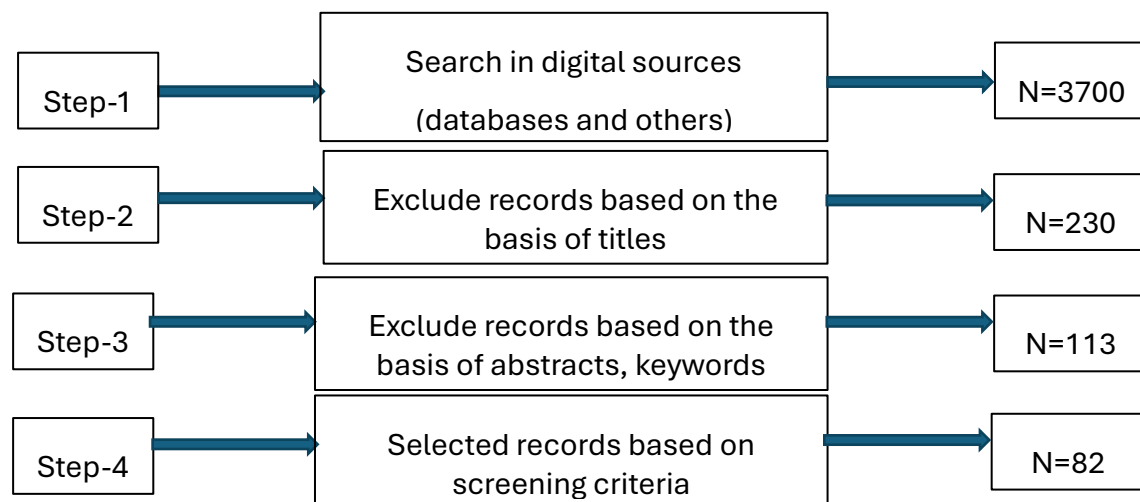


Figure 3. 2 The selection process of Data Governance and Dark Data Governance Sources

Nature of Contribution	Format	Study
Academic	Papers in journals and conference proceedings, books, working	DG: (40 references) (Price, R. and Shanks, G., 2004), (Weber, K., Otto, B. and Osterle, H., 2009) , (Olaitan, O., Herselman, M. and Wayi, N., 2016) , (DAMA., 2017) , (Khatri, V. and Brown, C., 2010) , (Otto, B., 2011), (Bruck, C., 2017) , (Abraham, R., Schneider,

	reports and theses.	J. and Brocke, v, J., 2019), (Otto, B., 2011), (Yebeles, J. and Zorrilla, M., 2019) , (Benfeldt, O., 2017) , (Al-Ruithe, M., Benkhelifa, E. and Hameed, K., 2016) , (Wende, K., 2007) , (Price, R. and Shanks, G., 2005) , (Wang, Y, R. and Strong, M, D., 1996) , (Ning, Z., 2016) , (Kooper, M., Maes, R. and Lindgreen, R, E., 2011) , (Acero, R, Á., Gonzales, A. and Raymundo, C., 2019) , (Arisandi, D. and Khudri, Y, M, T., 2021) , (Jagals, M. and Karger, E., 2021) , (Cheong, K, L. and Chang, V., 2007) , (Maniezzo, V. and Colorni, A., 1999) , (Baškarada, S., Gao, J. and Koronios, A., 2006) , (Lee, W, Y. et al., 2002) , (Permana, I, R. and Suroso, S, J., 2018) , (Guetat, A, B, S. and Dakhli, D, B, S., 2015), (Gelbstein, E., 2017) , (Côte-Real, N., Ruivo, P. and Oliveira, T., 2020), (Thiel, R., Stroetmann, K. and Singleton, P., 2014), (Mento, A., 2002) , (Al-Ruithe, M. and Benkhelifa, E., 2017) , (Borgman, P, H. et al., 2016), (Alreemy, Z. et al., 2016) , (AlGhamdi, S., Win, T, K. and Vlahu-Gjorgievska, E., 2020) , (Hagmann, J., 2013) , (Loshin, D., 2010), (Bruin, D, R. and Solms, v, S., 2015) , (Cheng, G. et al., 2017) , (Brous, P., Janssen, M. and Vilminko-Heikkinen, R., 2016) , (Niemi, E. and Laine, S., 2016) Dark DG: (17) (Karande, A. et al., 2019) , (Hand, J, D., 2020), (Veaux, D, D, R. and Hand, J, D., 2005) , (Purss, B, M. et al., 2015), (Ajis, M, F, A. and Baharin, H, S., 2019) , (Sundarraj, M. and Natrajan, M, R., 2019) , (Gimpel, G., 2020), (Wiebe, H, P. and Allison, D, M., 2015) , (Gallaher, W, D. et al., 2015) , (Kim, W. et al., 2003) , (Provost, J. and Danyluk, A., 1995) , (Trajanov, D. et al., 2018), (Heidorn, B, P., 2008), (Jagadish, H., 2022), (Lavallo, S. and Smilde, S., 2021), (Sun, Z., Su, T. and Shen, Y., 2023), (Xia, Y., Yao, H. and Zhang, M., 2022)
Practice-Oriented	Publications by industry associations, software vendors, analysts, and consultants	DG: (11 references) (Thomas, G., 2020), (Judah, S. and White, A., 2021) , (Collibra., 2020), (HNU., 2020) , (Curtiss, J., Saxena, S. and Seth, A., 2018), (Agarwal, M., 2021), (Stedman, G. and Vaughan, J., 2020) , (Snowflake, D., 2019) , (Cafarella, M. et al., 2016) , (Everett, D., 2019), (Hinkle, O., 2020) Dark DG: (14 references)

		(Redman, T., 2016), (Marus, P., 2018), (Gartner., 2020) , (Deloitte, P, U., 2017), (Splunk., 2019), (McNulty, K., 2017) , (Meghji, S., 2017) , (Agrawal, S., 2019) , (Marsh, S., 2019), (Redman, C, T., 2018), (Rees, V, I., 2020) , (Johnson, J., 2020) , (Cheng, S., 2018), (York, T., 2023)

Table 3. 4 Categorization of sources on data governance as per search protocol

3.7. Results and Analysis

This section presents and discusses the findings of the systematic review conducted to examine the state of research on data governance and dark data governance. The review identified 82 relevant studies across various publication formats, including surveys, industry reports, case studies, and academic frameworks and models. These studies were thoroughly analysed to capture the breadth of research topics within the data governance and dark data governance domains. The literature review spanned publications from 1995 to 2023, encompassing both academic and practice-oriented sources.

The studies were categorized into two main groups:

- research on the state of the art in data governance, and
- research on the state of the art in dark data governance.

The results are presented and discussed in relation to the publication year and the nature of the contribution (academic or practice-oriented). These findings are explored in detail in the subsequent sections.

3.7.1. Publication Year

Figure 3.3 presents a pie chart that illustrates the distribution of sources across different categories, with the precise number of sources included in each category label. This visual representation offers a clear perspective on both the percentage breakdown and the exact quantities of sources in the "Academic DG," "Academic Dark DG," "Practice-Oriented DG," and "Practice-Oriented Dark DG" categories.

Figure 3.4 presents a stacked bar chart depicting the chronological distribution of the sources included in the systematic review. The chart categorizes the sources by their nature of contribution, distinguishing between academic and practice-oriented literature, as well as their focus area on data governance or dark data governance. This visualization provides an overview of the publication trends across the different domains over the years covered in the

study, offering insights into the evolving research landscape and the balance between academic and industry perspectives in these important areas of data management.

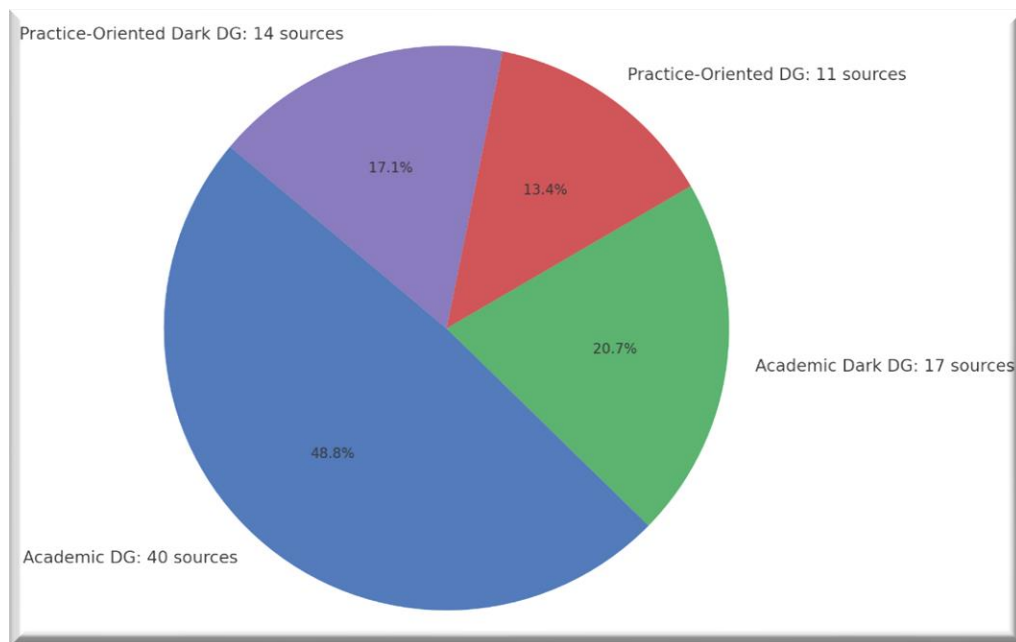


Figure 3. 3 Distribution of Sources by Nature of Contribution

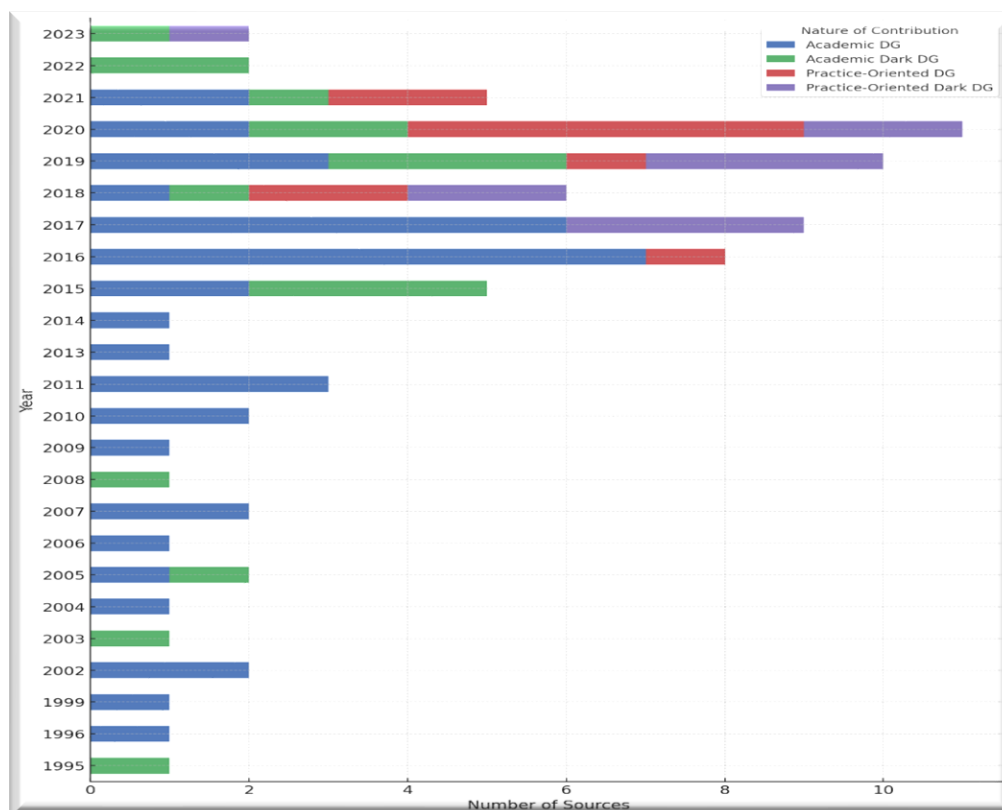


Figure 3. 4 The distribution of sources over the studied years

Figure 3.5 presents a stacked bar chart that displays the chronological distribution of the sources included in the systematic review for the "Academic DG" and "Practice-Oriented DG" categories. This visualization provides a detailed breakdown of the publication trends over the years, illustrating the relative contributions from academic and practice-oriented research on data governance. The stacked bars allow for easy comparison of the volume and growth patterns between the two categories. This visualization offers insights into the publication trends and relative emphasis in this study, highlighting the balance between academic and industry-oriented research on data governance across the time period examined.

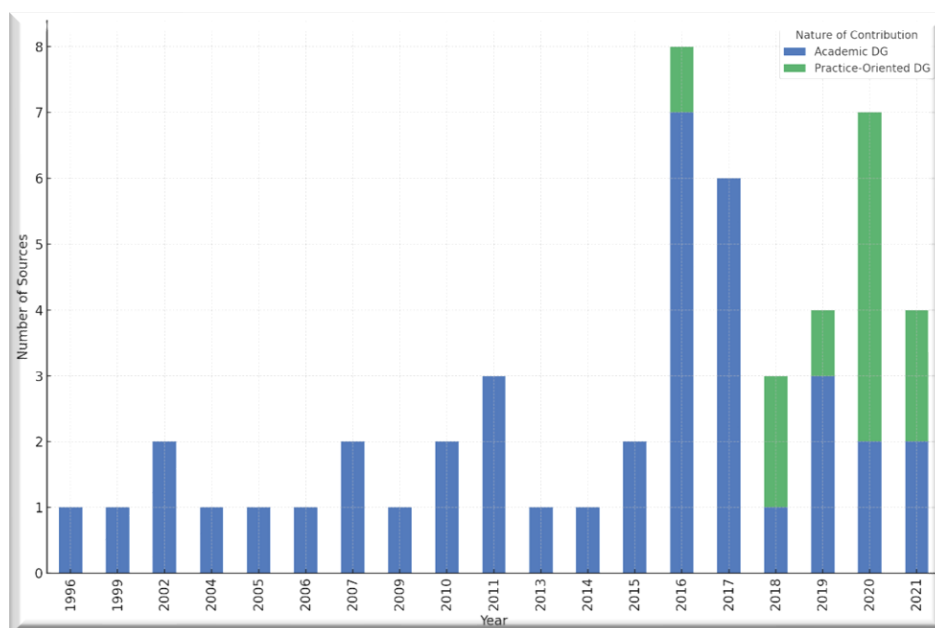


Figure 3. 5 The distribution of DG sources over the studied years for data governance

Figure 3.6 presents a stacked bar chart depicting the chronological distribution of the sources included in the systematic review, categorized by their academic or practice-oriented nature. This visualization offers insights into the publication trends over the years, highlighting the relative emphasis and contributions from the academic and industry sectors in the domain of dark data governance. The stacked bar chart format facilitates a clear comparative analysis of the volume between the two categories, offering an overview of the research landscape in this specific domain.

3.7.2. Nature of Contribution

This section explores the distribution of sources based on the nature of their contribution - whether they originate from academic or practice-oriented literature during the period 1995-2023. The analysis provides a deeper understanding of the balance between theoretical research

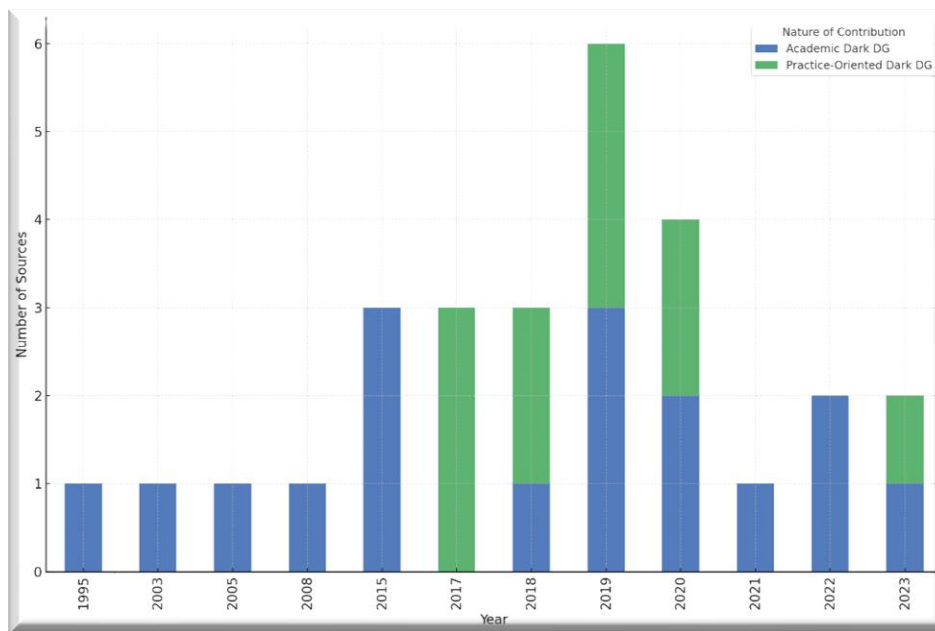


Figure 3. 6 The distribution of Dark DG sources over the studied years for dark data governance

and industry-driven perspectives within the data governance and dark data governance domains.

Figure 3.7 presents a bar chart displaying the number of sources per year across the four distinct categories: Academic Data Governance, Academic Dark Data Governance, Practice-Oriented Data Governance, and Practice-Oriented Dark Data Governance. This visualization offers a comprehensive overview of the publication trends and relative emphasis in these domains, highlighting both academic and industry-focused contributions over the time period examined. Figure 3.8 below presents a detailed breakdown of the number of sources per year for the two data governance categories: Academic Data Governance and Practice-Oriented Data Governance. This visualization offers a clear comparison of the publication trends and relative emphasis by this study between the academic and industry-focused literature on data governance over the time period examined.

Figure 3.9 below presents a bar chart displaying the number of sources per year for the "Academic Dark DG" and "Practice-Oriented Dark DG" categories. This visualization offers a detailed breakdown of the publication trends over the years, highlighting the relative contributions from academic and practice-oriented research on the topic of dark data governance. The bar format allows for comparison of the volume between the two categories, providing a clear picture of this research landscape in this specific domain.

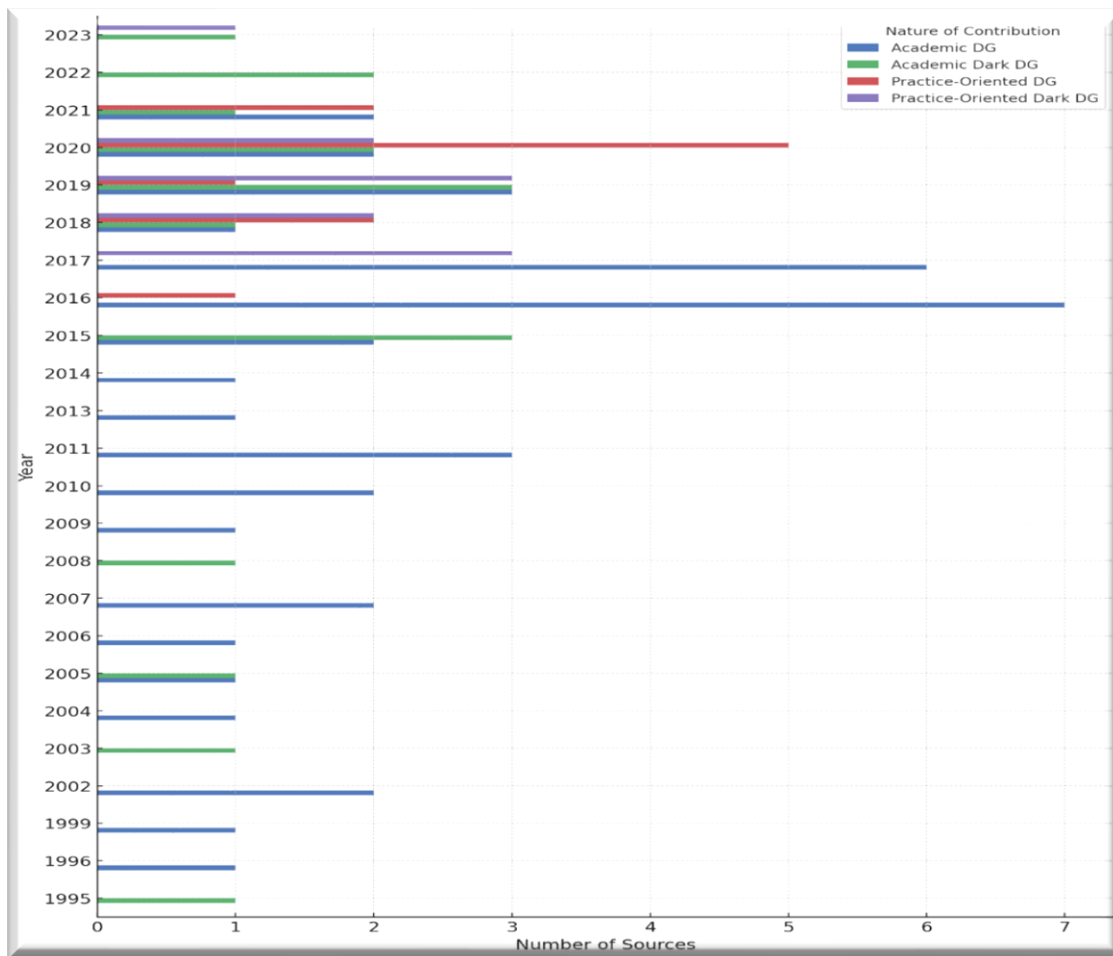


Figure 3. 7 The number of all sources is based on the nature of the contribution.

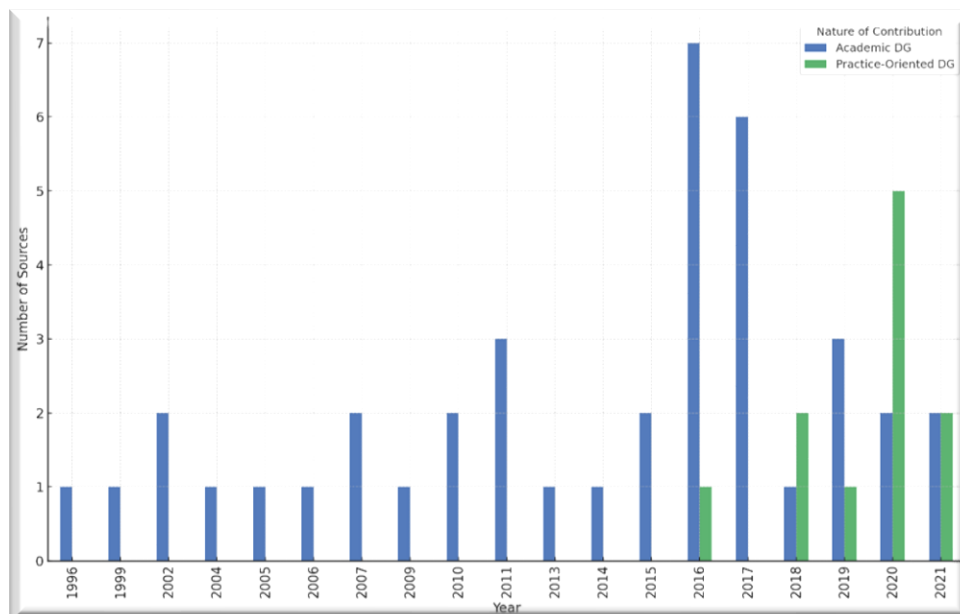


Figure 3. 8 The number of Sources of data governance is based on the nature of the contribution.

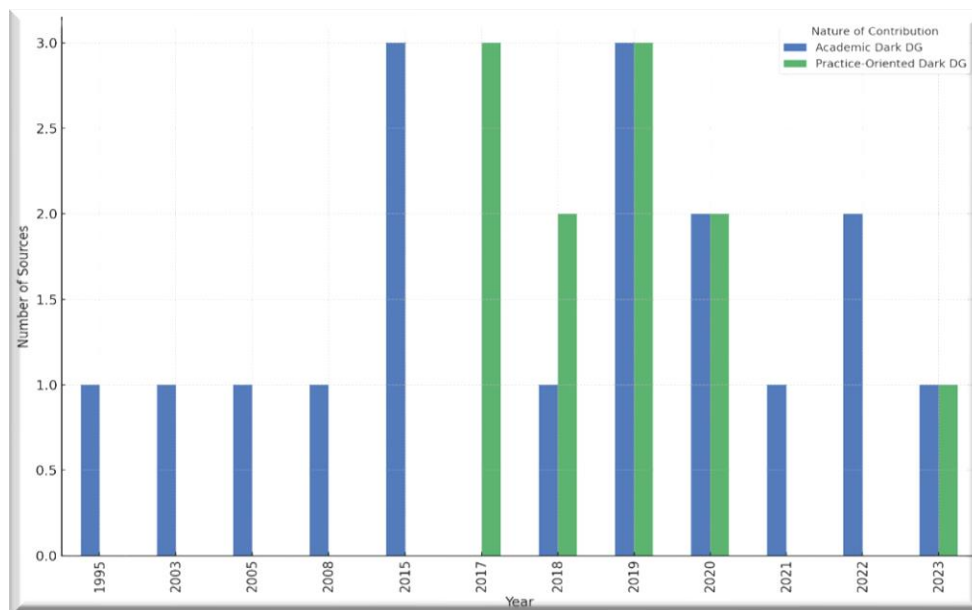


Figure 3. 9 The number of sources of dark data governance based on the nature of the contribution.

3.7.3. Analysis of the State of the Art for Data Governance and Dark Data Governance

According to the review protocol described in Section 3.5, the search results identified 82 records addressing the area of data governance and dark data governance, 40 scientific data governance records and 11 practice-oriented data governance records, 17 scientific dark data governance records, and 14 practice-oriented dark data governance records. Table 3.5 presents a detailed summary of the key findings from each of the 82 sources included in the literature review on data governance and dark data governance. This table provides an overview of the main contributions, and conclusions drawn in the reviewed studies. It covers both academic publications, such as journal articles and conference papers, as well as practice-oriented sources, like industry reports and white papers. By summarizing the core insights from this comprehensive set of sources, Table 3.5 offers a comprehensive snapshot of the current state of research and practice in the areas of data governance and dark data governance.

Source Name	Authors	Main Conclusions
Data Governance: A Conceptual Framework, Structured Review, and Research Agenda	Abraham, Schneider & Brocke (2019)	Proposes a six-dimensional framework for data governance, identifying key components and gaps in the literature.

Source Name	Authors	Main Conclusions
Designing Data Governance	Khatri & Brown (2010)	Presents a framework focusing on data as an asset, with five key decision domains: Data Principles, Quality, Metadata, Access, and Lifecycle.
A Morphology of The Organisation of Data Governance	Otto (2011)	Proposes a structure for organizing data governance, focusing on decision rights in various organisational forms (centralized, decentralized, virtual).
One Size Does Not Fit All—A Contingency Approach to Data Governance	Weber, Otto & Osterle (2009)	Recommends tailoring data governance frameworks to fit specific organisational needs and configurations.
DAMA-DMBOK (Data Management Body of Knowledge)	DAMA (2017)	Defines data governance within the broader scope of data management, emphasizing processes, people, and technology.
Data Governance Institute	Thomas (2020)	Organises data governance around purpose, actions, participants, and process value.
Key Dimensions for Cloud Data Governance	Al-Ruithe, Benkhelifa & Hameed (2016)	Highlights data governance challenges in cloud environments and proposes a framework addressing privacy, security, and compliance.
A Comprehensive Review of Data Governance Literature	Benfeldt (2017)	Calls for more practical data governance applications, especially in the public sector.
A Model for Data Governance – Organizing Accountabilities for Data Quality Management	Wende (2007)	Focuses on organizing responsibilities in data quality management to improve governance effectiveness.

Source Name	Authors	Main Conclusions
A Semiotic Information Quality Framework	Price & Shanks (2004)	Proposes a framework for information quality based on syntactic, semantic, and pragmatic categories.
Empirical Refinement of a Semiotic Information Quality Framework	Price & Shanks (2005)	Empirically refines a semiotic framework, highlighting how syntactic, semantic, and pragmatic dimensions impact information quality and suggesting improvements for data governance and quality assurance.
Beyond Accuracy: What Data Quality Means to Data Consumers	Wang & Strong (1996)	Expands data quality beyond accuracy, focusing on dimensions like timeliness and completeness for user needs.
Dark Data, Why What You Don't Know Matters	Hand (2020)	Categorizes dark data into 15 types and proposes governance strategies centred on awareness and risk management.
IT Glossary: Dark Data	Gartner (2020)	Defines dark data as underutilized information assets, emphasizing the risks and costs of storage without value extraction.
Bringing Dark Data Into the Light: Illuminating Existing IoT Data Lost Within Your Organisation	Gimpel (2020)	Identifies two types of dark data (unknown and partially visible) and proposes strategies to unlock value through its governance.
Towards a Data Governance Framework for Third-Generation Platforms	Yebeles & Zorrilla (2019)	Develops a data governance framework for cloud-based and big data platforms, addressing privacy and compliance challenges.
Dark Data Management as a Frontier of Information Governance	Ajis & Baharin (2019)	Proposes strategies for leveraging dark data in decision-making and improving business outcomes.
Bringing Dark Data Into the Light: A Case Study of the Recovery of Northwestern Atlantic Zooplankton Data	Wiebe & Allison (2015)	Highlights the recovery of historical data through a dark data governance model, focusing on infrastructure and metadata for data discoverability.

Source Name	Authors	Main Conclusions
Taxonomy of Literature to Justify Data Governance as a Prerequisite for Information Governance	Olaitan, Herselman & Wayi (2016)	Argues for data governance as foundational to information governance, categorizing key studies supporting this view.
The State of Dark Data	Splunk (2019)	Identifies challenges and strategies for unlocking dark data value through proper governance and technology.
How to Lie With Bad Data	Veaux & Hand (2005)	Discusses bad data manipulation and proposes management techniques focusing on metadata, profiling, and AI for quality improvement.
Importance of Dark Data and its Applications	Karande et al. (2019)	Focuses on structuring and analysing unstructured dark data, particularly in finance, for better decision-making.
Expanding the Definition of Dark Data and Mining It With Dark Analytics	McNulty (2017)	Expands dark data definition and introduces "dark analytics" for analysing inaccessible data.
The process of bringing dark data to light: The rescue of the early Nimbus satellite data	Gallaher et al. (2015)	Discusses data recovery strategies and proposes infrastructure upgrades for dark data preservation.
A Sustainable Method to Handle Dark Data in a Smart Factory	Sundarraaj & Natrajan (2019)	Proposes integrating unstructured dark data into smart factory processes for optimization and better data governance.
An Overview of Data Governance	Ning (2016)	Outlines key components of data governance like policies, roles, and responsibilities for ensuring quality and compliance.
Data is Holding Back AI (Impact of Dark Data)	Meghji (2017)	Highlights how poor data management hampers AI development, stressing the need for data quality improvement.

Source Name	Authors	Main Conclusions
A Taxonomy of Dirty Data	Kim et al. (2003)	Provides a taxonomy of dirty data and proposes data quality enhancement techniques for managing dark data.
Transforming Data Into Action: The Business Outlook for Data Governance	Curtiss, Saxena & Seth (2018)	Discusses how organisations can leverage data governance for actionable insights, focusing on continuous data access improvement and aligning data strategies with business objectives.
Hype Cycle for Data and Analytics Governance and Master Data Management	Judah & White (2021)	Proposes a connected governance framework to address complex business challenges across organisations.
Bad Data Costs the U.S. \$3 Trillion Per Year	Redman (2016)	Discusses the financial impact of poor data quality and proposes data governance solutions for cost reduction.
CIOs Can Harness Dark Data to Boost Innovation	Agrawal (2019)	Proposes strategies to unlock innovation and customer experience improvements by managing dark data effectively.
Dark Data – The Blind Spots in Your Analytics	Marsh (2019)	Explains how dark data creates blind spots in analytics and suggests strategies to unlock its value.
Dark Analytics: Illuminating Opportunities Hidden Within Unstructured Data	Deloitte (2017)	Introduces dark analytics as a method for exploiting untapped unstructured data and emphasizes the need for competent people.
If Your Data Is Bad, Your Machine Learning Tools Are Useless	Redman (2018)	Emphasizes the importance of data quality in machine learning for accurate predictions.
Dark Data: A Complex Challenge for Enterprises and CIOs in the Cloud Era	Marus (2018)	Focuses on dark data management challenges in cloud environments, recommending investments in storage and infrastructure with clear policies.

Source Name	Authors	Main Conclusions
Inter-Organisational Data Governance: A Literature Review	Jagals & Karger (2021)	Proposes a framework for inter-organisational data governance, focusing on structure, processes, and compliance.
Learning from Bad Data	Provost & Danyluk (1995)	Highlights strategies for improving machine learning accuracy when dealing with poor data.
On the governance of information: Introducing a new concept of governance to support the management of information	Kooper, Maes & Lindgreen (2011)	Proposes a holistic, adaptable information governance model integrating data management, security, and compliance to support evolving business needs.
The Evolution of Dark Data and How It Makes Your Business Smarter	Rees (2020)	Discusses how dark data can be transformed into valuable insights to drive business innovation.
The Need for Data Governance: A Case Study	Cheong & Chang (2007)	Emphasizes the importance of data governance for managing quality and compliance (e.g., Sarbanes-Oxley Act), highlighting challenges in defining roles and ensuring collaboration between IT and business.
Collibra - What is Data Governance and Why Does it Matter?	Collibra (2020)	Highlights the role of data governance in enabling collaboration, ensuring compliance, and improving data quality, consistency, and security, helping organisations become more data-centric.
The Impact of Data Quality Information on Decision Making: An Exploratory Analysis	Maniezzo & Colorni (1999)	Stresses the importance of reliable data for decision-making, showing how poor data quality impacts accuracy, completeness, and timeliness, affecting organisational confidence and outcomes.
What Is Dark Data? The Basics & The Challenges	Johnson (2020)	Defines dark data as unanalysed, unstructured data, highlighting privacy concerns, challenges in management, and risks alongside opportunities if not managed correctly.

Source Name	Authors	Main Conclusions
Agile Maturity Model Approach to Assessing and Enhancing the Quality of Asset Information in Engineering Asset Management Information Systems	Başkarada, Gao & Koronios (2006)	Proposes a maturity model for improving the quality of asset information management, progressing from chaotic to optimized stages, and addressing issues like data collection, management, and exploitation.
AIMQ: A Methodology for Information Quality Assessment	Lee et al. (2002)	Provides a structured approach to assessing information quality, focusing on intrinsic, contextual, and representational dimensions to ensure organisational data meets user needs.
Data Governance Maturity Model	HNU (2020)	Describes a five-level data governance maturity model based on SEI's Capability Maturity Model, offering a roadmap for organisations to develop mature governance processes.
Data Governance Reference Model under the Lean Methodology for the Implementation of Successful Initiatives in the Peruvian Microfinance Sector	Acero, Gonzales & Raymundo (2019)	Proposes a data governance model using the Lean methodology, tailored to address unique challenges in microfinance, validated through a case study to improve governance practices.
Challenges and Opportunities of Data Governance in Private and Public Organisations	Bruck (2017)	Explores data governance challenges like ownership and regulatory compliance in both private and public sectors, emphasizing improved decision-making and operational efficiency.
Organizing Data Governance: Findings from the Telecommunications Industry and Consequences for Large Service Providers	Otto (2011)	Examines data governance practices in telecoms, identifying challenges such as large data volumes and regulatory compliance, while stressing collaboration between IT and business units.
The Architecture Facet of Information Governance:	Guetat & Dakhli (2015)	Focuses on the importance of aligning data architecture with governance frameworks

Source Name	Authors	Main Conclusions
The Case of Urbanized Information Systems		to ensure data integrity, security, and compliance.
IS Audit Basics: Data Management Body of Knowledge (DMBOK)	Gelbstein (2017)	Summarizes DMBOK for auditors, emphasizing data governance, quality, and auditing the effectiveness of data management practices.
Dark Data in Internet of Things: Challenges and Opportunities	Trajanov et al. (2018)	Discusses dark data challenges in IoT, offering strategies for managing unstructured data to unlock business opportunities and operational efficiency.
Leveraging internet of things and big data analytics initiatives in European and American firms: Is data quality a way to extract business value?	Côrte-Real, Ruivo & Oliveira (2020)	Confirms that better data quality is needed to unlock the potential of IoT and Big Data Analytics, improving decision-making and user productivity.
Clinical Data Governance: Legal and Ethical Challenges	Thiel, Stroetmann & Singleton (2014)	Explores the legal and ethical challenges in clinical data governance, particularly regarding privacy, data protection, and anonymization under the European Data Protection Directive.
Top 3 Challenges for Data & Analytics Leaders	Agarwal (2021)	Identifies top challenges for data leaders, such as improving data literacy, measuring the value of data initiatives, and balancing agility with governance.
Shedding Light on the Dark Data in the Long Tail of Science	Heidorn (2008)	Discusses the underutilization of large scientific datasets and suggests strategies for managing dark data to enhance scientific discovery and innovation.
A Change Management Process: Grounded in Both Theory and Practice	Mento (2002)	Proposes a structured approach to managing organisational change, aligning initiatives with goals.
Dotting the I and Crossing (Out) the T in IT Governance: New Challenges for Information Governance	Borgman et al. (2016)	Explores challenges in information governance due to cloud services and cross-boundary data use, proposing a framework to address these issues.

Source Name	Authors	Main Conclusions
Critical Success Factors for Information Technology Governance (ITG)	Alreemy et al. (2016)	Identifies leadership and alignment with business strategy as key success factors for effective IT governance.
What Is Data Governance and Why Does It Matter?	Stedman & Vaughan (2020)	Defines data governance as the process of managing data availability, integrity, and security, ensuring consistency and compliance.
Information Security Governance Challenges and Critical Success Factors	AlGhamdi, Win & Vlahu-Gjorgievska (2020)	Proposes a holistic framework for information security governance, addressing challenges and critical success factors.
Analysis and Classification of Barriers and Critical Success Factors for Implementing a Cloud Data Governance Strategy	Al-Ruithe & Benkhelifa (2017)	Analyses barriers to cloud data governance and identifies critical success factors for framework adaptation.
Analysis and Design of Data Governance at the Financial Services Authority	Arisandi & Khudri (2021)	Proposes a data governance framework tailored for financial institutions, focusing on regulatory compliance and data security, validated by the DAMA model (2017).
Three Ways Organisations Can Achieve Data Governance Success	Hinkle (2020)	Suggests involving the right people, simplifying processes, and tailoring technology to achieve successful data governance.
Information Governance - Beyond the Buzz	Hagmann (2013)	Discusses practical strategies for implementing effective information governance frameworks, focusing on data quality, privacy, and security, while also aligning with business objectives.
Five Steps to Successful Data Governance	Snowflake (2019)	Outlines a five-step approach to developing a successful data governance program, focusing on strategy, data control, and continuous improvement.

Source Name	Authors	Main Conclusions
Experts With Impact in Information Governance	Cheng (2018)	Highlights the risks associated with mishandling dark data and proposes strategies for managing large volumes of dark data to avoid legal and operational risks.
Coordinating Decision-Making in Data Management Activities: A Systematic Review of Data Governance Principles	Brous, Janssen & Vilminko-Heikkinen (2016)	Identifies four key data governance principles: organisation, alignment, compliance, and common understanding for coordinating decision-making in data management activities.
Dark Data: Are We Solving the Right Problems?	Cafarella et al. (2016)	Questions whether current efforts in dark data management address the right challenges, calling for new approaches to data curation and quality management.
Operationalizing Data Governance Through Data Policy Management	Loshin (2010)	Suggests that practical data governance requires well-defined policies aligned with business objectives to bridge the governance gap.
Unlocking the Australian Landsat Archive – From Dark Data to High Performance Data Infrastructures	Purss et al. (2015)	Describes the migration of Australia's Landsat archive to high-performance infrastructures, transforming dark data into valuable resources for research applications.
Data Governance vs. Data Management: What's the Difference?	Everett (2019)	Distinguishes data governance as the framework for managing the data lifecycle and data management as the technical execution of governance policies.
Designing Information Governance with a Focus on Competence Management in a Knowledge-Intensive Project Organisation	Niemi & Laine (2016)	Proposes treating information as a strategic asset and integrating competence management to optimize its use for competitive advantage.
Data Governance Maturity Assessment at PT. XYZ: Case Study on Data Management Division	Permana & Suroso (2018)	Uses the Stanford Model to assess the maturity of data governance in an organisation, outlining a path from informal to fully integrated governance practices.

Source Name	Authors	Main Conclusions
Modelling Cyber Security Governance Maturity	Bruin & Solms (2015)	Proposes a cybersecurity governance maturity model focused on leadership, risk management, and continuous improvement.
Cloud Data Governance Maturity Model	Cheng et al. (2017)	Introduces a maturity model for assessing and improving cloud data governance practices, aligned with business strategy.
Dark Data: Discovery, Uses & Benefits of Hidden Data	York (2023)	Discusses the potential value of dark data and how it can improve decision-making, operational efficiency, and risk management when properly governed.
Data Management and Dark Data: New Challenges and Opportunities	Jagadish (2022)	Suggests using advanced analytics and machine learning to detect and manage dark data, integrating it into broader data governance models.
The Governance of Dark Data: New Frontiers in Data Management	Lavalle & Smilde (2021)	Proposes a governance framework for managing dark data, including data classification, risk assessment, and lifecycle management.
Dark Data in Organisations: Risks, Governance Strategies, and Case Studies	Sun, Su & Shen (2023)	Presents a governance model integrating dark data management into broader data governance strategies, emphasizing risk management and value creation.
Governance of Dark Data in the Era of Big Data: A Critical Review	Xia, Yao & Zhang (2022)	Proposes an enhanced framework for governing dark data, incorporating automated discovery tools, data stewardship, and metadata management

Table 3. 5 The main findings of each Source

The roots of data governance research can be traced back to the early 1980s; however, the first efforts to propose a framework for data governance were published in 2007 (Niemi, E., 2011). Niemi (2011) also observed that all existing sources for data governance from researchers and practitioners, at the time he published his paper, focused on the placement of decision-making authority for Data Quality Management (DQM) and organisational structuring. The discussion on data governance and dark data governance reflects the evolution of thought and practice in managing organisational data assets, with significant contributions made over the past two

decades. The earliest work among the selected references, by Wang and Strong (1996), laid the groundwork by broadening the concept of data quality beyond mere accuracy, considering dimensions such as timeliness, completeness, and relevance, which are crucial for ensuring that data meets the specific needs of its users. This foundational understanding of data quality set the stage for more comprehensive frameworks of data governance that emerged in the following years. By 2007, Wende's work on data governance ("A Model for Data Governance – Organizing Accountabilities for Data Quality Management") introduced a model focusing specifically on data quality management (DQM). Wende identified key decision areas and roles involved in DQM, proposing a matrix to assign responsibilities within an organisation. This model was instrumental in structuring data governance practices to ensure high data quality standards, reflecting an early recognition of the importance of governance in managing data quality systematically. Wende (2007), suggested also, transferring knowledge to build IT governance into the development of data governance initiatives. In 2009, Weber, Otto, and Osterle took the discourse a step further by presenting a contingency approach to data. Their paper argued against a universal approach to data governance, instead advocating for a model that tailors the governance framework to the specific needs of an organisation. This approach was particularly relevant as organisations began to encounter increasingly diverse and complex data environments, where a flexible and context-specific governance model was necessary to align data management with organisational objectives (Figure 3.10).

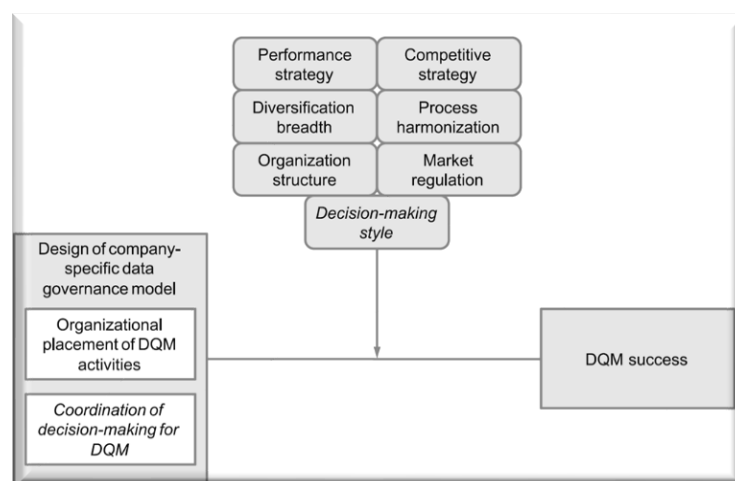


Figure 3. 10 Contingency Approach to DG

Khatri and Brown (2010) further advanced the field by emphasizing the strategic importance of data governance in their work regarding designing data governance. They provided a comprehensive framework focused on five key decision domains: Data Principles, Data

Quality, Metadata, Data Access, and Data Lifecycle. Their framework was designed to guide organisations in aligning data governance with IT governance, thereby ensuring that data management practices not only support but also enhance organisational goals. This work highlighted the critical need for organisations to treat data as a strategic asset, a theme that has become increasingly central to discussions of data governance (Table 3.6).

Data Governance Domains	Domain Decisions	Potential Roles or Locus of Accountability
Data Principles • Clarifying the role of data as an asset	• What are the uses of data for the business? • What are the mechanisms for communicating business uses of data on an ongoing basis? • What are the desirable behaviors for employing data as assets? • How are opportunities for sharing and reuse of data identified? • How does the regulatory environment influence the business uses of data?	• Data owner/trustee • Data custodian • Data steward • Data producer/supplier • Data consumer • Enterprise Data Committee/Council
Data Quality • Establishing the requirements of intended use of data	• What are the standards for data quality with respect to accuracy, timeliness, completeness and credibility? • What is the program for establishing and communicating data quality? • How will data quality as well as the associated program be evaluated?	• Data owner • Subject matter expert • Data quality manager • Data quality analyst
Metadata • Establishing the semantics or "content" of data so that it is interpretable by the users	• What is the program for documenting the semantics of data? • How will data be consistently defined and modeled so that it is interpretable? • What is the plan to keep different types of metadata up-to-date?	• Enterprise data architect • Enterprise data modeler • Data modeling engineer • Data architect • Enterprise Architecture Committee
Data Access • Specifying access requirements of data	• What is the business value of data? • How will risk assessment be conducted on an ongoing basis? • How will assessment results be integrated with the overall compliance monitoring efforts? • What are data access standards and procedures? • What is the program for periodic monitoring and audit for compliance? • How is security awareness and education disseminated? • What is the program for backup and recovery?	• Data owner • Data beneficiary • Chief information security officer • Data security officer • Technical security analyst • Enterprise Architecture Development Committee
Data Lifecycle • Determining the definition, production, retention and retirement of data	• How is data inventoried? • What is the program for data definition, production, retention, and retirement for different types of data? • How do the compliance issues related to legislation affect data retention and archiving?	• Enterprise data architect • Information chain manager

Table 3. 6 DG domains including domain decisions and potential roles

Otto (2011) reported that organisations that believe they have a data governance programme in fact have not considered all the aspects required for these programmes to be complete and effective. This work was the only attempt in the literature to review the area of data governance, up until 2010. It aimed to develop a morphology of data governance organisation. This study contributed significantly to understanding how data governance can be organised within companies. Otto focused on the assignment of decision rights and responsibilities, developing a morphology that considered different organisational forms (centralized, decentralized, virtual) and roles (such as data stewards and data governance councils). His work provided

both a theoretical and practical framework, validated through case studies, offering organisations a structured approach to tailoring their data governance structures to their specific operational needs (Figure 3.11).

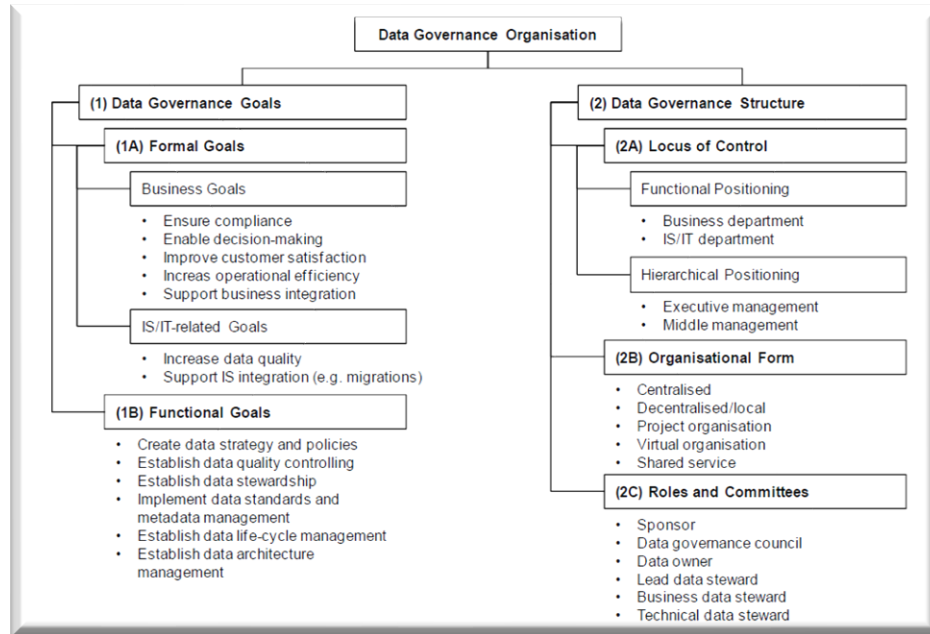


Figure 3. 11 Data Governance Morphology – DG Goals and DG Structure

In 2016, Al-Ruithe, Benkhelifa, and Hameed addressed the emerging challenges of data governance in cloud environments. They proposed a governance framework tailored to the unique demands of cloud computing, emphasizing critical dimensions such as data ownership, data protection strategies, and service level agreements (SLAs). This work was particularly important as organisations increasingly adopted cloud-based services, which introduced new complexities in data management, such as issues of data privacy, security, and regulatory compliance. Data governance, as outlined by DAMA (DAMA., 2017), is the structured exercise of authority over data management, focusing on ensuring data quality, compliance, and security across an organisation. It involves establishing policies, standards, and roles, such as data stewards, to manage data effectively, aligning with business objectives, and fostering a culture of responsible data use. The framework emphasizes the importance of strategic alignment, continuous monitoring, and the integration of tools and technology to support governance efforts. Effective data governance leads to improved data quality, regulatory compliance, better decision-making, and operational efficiency, with a focus on evolving and adapting the governance program over time (Figure 3.12).

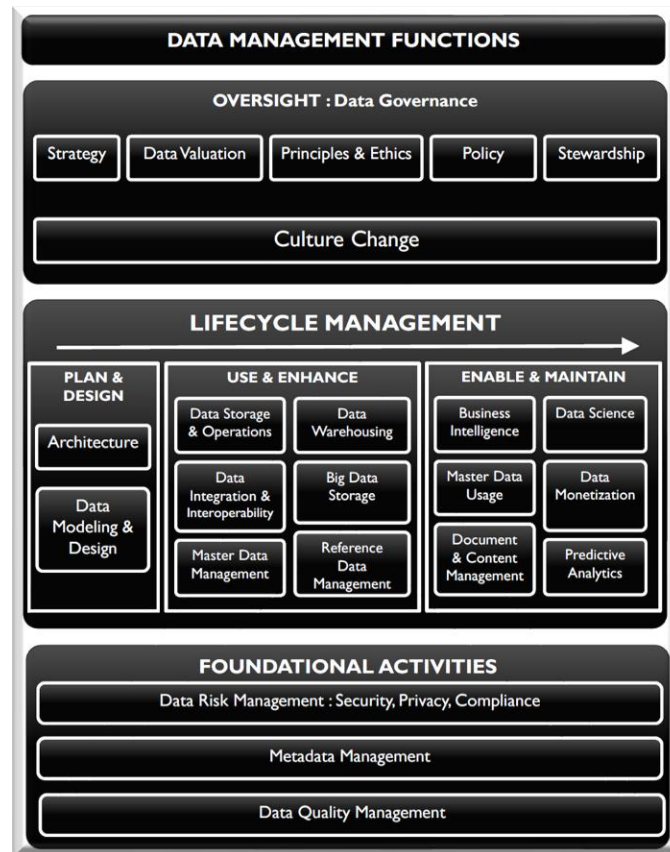


Figure 3. 12 Data Governance within Data Management Context (DAMA, 2017)

The article by Abraham, Schneider, and Brocke (2019) provides a comprehensive examination of the data governance field, presenting a conceptual framework that integrates various governance mechanisms, organisational scopes, and data scopes. The framework is designed to guide both researchers and practitioners in understanding and implementing effective data governance strategies across different organisational contexts. The article emphasizes the importance of aligning data governance with organisational objectives, ensuring that data is managed consistently and effectively throughout its lifecycle. This study is significant in the progression of the data governance field, as it presents a comprehensive framework that integrates technical, organisational, and strategic dimensions of data management, while accounting for the organisational and environmental factors that shape the setup and configuration of data governance practices (Figure 3.13).

Data governance, as outlined by the Data Governance Institute (DGI), is the system of decision rights and accountabilities for managing data as an enterprise asset (Thomas, G., 2020), (DGI., 2024). It involves the formal orchestration of people, processes, and technology to ensure that data is properly managed, used, and protected across an organisation. DGI emphasizes the creation of a framework that defines who is responsible for data-related decisions and how

The existing literature suggests that implementing robust data governance can enhance data utilization by improving various dimensions of data quality, such as accuracy, availability, completeness, consistency, and timeliness. Moreover, data governance frameworks can help organisations mitigate data-related errors and inconsistencies (Abraham, R., Schneider, J. and Brocke, v, J., 2019). Researchers have argued that key organisational factors influence the positioning of data quality management and thereby impact its successful implementation. Furthermore, the same study contends that the organisation's decision-making style shapes the relationship between the coordination of decision-making activities and the successful delivery of data quality management (Weber, K., Otto, B. and Osterle, H., 2009). The primary objective of data governance is to facilitate the successful support of data production and utilization, ensuring that foundational data-related activities (e.g. data quality management) are carried out in a disciplined manner. Furthermore, data governance enables organisations to become more data-driven, empowering them to recognize and act upon opportunities to derive value from their data assets (DAMA., 2017). The primary objective of data governance is to enhance data quality. Effective data governance must be aligned with and driven by the organisation's strategic business objectives (Benfeldt, O., 2017). Research has shown that effective enterprise-wide data management may not be achievable without formal data governance. Data governance provides a structured framework to mitigate data management risks. It also enables the alignment of data-related programs with corporate objectives and facilitates cross-organisation collaboration (Cheong, K, L. and Chang, V., 2007). According to DAMA, effective data governance improves data quality (DAMA., 2017). Additionally, the Data Governance Institute stated that the primary goal of data governance is to ensure that data is accurate, available, secure, and aligned with the organisation's strategic objectives. This, in turn, enables better decision-making, regulatory compliance, and effective risk management (Thomas, G., 2020), (DGI., 2024).

Based on the above, the existing literature emphasizes the primary objectives of data governance in improving data quality and mitigating data-related risks. However, the discussion of dark data governance, a more recent development within the broader field of data governance, has gained prominence in the late 2010s and early 2020s. This reflects organisations' growing recognition of the potential value in the data they have collected but lacked quality checks or remained unutilized. Lavalley and Smilde (2021) proposed a data governance framework specifically designed to address the challenges of dark data. Their framework emphasized the importance of data classification, risk assessment, and lifecycle management, and stressed the need to align dark data governance with broader organisational

objectives. This approach was critical in ensuring that dark data, often seen as a liability, could be managed in a way that added value while mitigating associated risks. Jagadish (2022) continued this exploration of dark data governance in his article. Jagadish suggested incorporating advanced analytics and machine learning into governance models to automatically detect and manage dark data. Jagadish emphasized the need for continuous monitoring and updating of data governance policies to adapt to the ever-evolving data landscape, highlighting the dynamic nature of dark data governance and the ongoing need for innovation and adaptation in this area. Sun, Su, and Shen (2023), in their paper proposed a governance model that integrates dark data management into broader organisational strategies. Their model was built around three main pillars: risk management, compliance, and value creation. By providing specific strategies for identifying, cataloguing, and securely storing dark data, their work ensured that dark data was not only stored securely but also made accessible and usable for decision-making processes. This confirms the growing recognition of dark data as a valuable resource within organisations, one that requires careful governance to unlock its full potential. Finally, Xia, Yao, and Zhang (2023) critically reviewed existing data governance models and proposed enhancements specifically for the governance of dark data in the era of big data. They integrated traditional data governance practices with new techniques for handling the volume, variety, and velocity of dark data. Their model aims to improve the visibility and governance of dark data within organisations, offering practical solutions for managing the complexities associated with modern data environments. Moreover, they suggested that the emerging challenges of big data and dark data governance suggest a need for more dynamic and adaptive governance models that can evolve with technological advancements and changing regulatory landscapes (Xia, Yao & Zhang, 2023).

This chronological overview illustrates the progression of thought in the field of data governance, encompassing both academic and practice-oriented perspectives. The discussion has evolved from early considerations of data quality and organisational frameworks to the more recent focus on the governance of dark data. This shift reflects the increasing complexity of data environments, driven by advancements in technology and the proliferation of data. As organisations struggle with the challenges of managing vast and varied data assets, the development of more sophisticated and context-specific governance models has become a necessity. These models aim to provide comprehensive solutions for effectively managing the growing volume, variety, and velocity of data, including the often-overlooked dark data, in order to unlock its full potential and support informed decision-making.

The governance frameworks discussed in this section highlight the lack of a unified approach to data governance and dark data governance, but this is not the only key challenge that causes confusion and failure in implementing effective data governance practices. As Bill Gates emphasized, "It's fine to celebrate success but it is more important to heed the lessons of failure". While acknowledging and reflecting on successes is valuable, it is of greater significance to devote attention to understanding and applying insights gained from failures. This highlights the need to carefully examine the reasons behind the shortcomings and failures of data governance initiatives, in order to learn from them and develop more robust and adaptable governance frameworks. Comprehending the key challenges and critical success factors is fundamental for organisations striving to overcome obstacles and harness the full strategic potential of data governance and dark data governance to ensure successful implementation. Analyses of the Key Challenges and Critical Success Factors are presented in the sections that follow.

3.7.4 Analysis of Key Challenges

Data governance programs often struggle or fail due to a variety of underlying challenges and obstacles. There are numerous reasons and contextual factors that contribute to the difficulties encountered in the implementation and maintenance of effective data governance initiatives. The literature suggests that data governance initiatives frequently encounter significant challenges that hinder their success. According to Gartner's prediction, 90% of organisations fail in their initial efforts to implement data governance (Correia, J., 2015). This high failure rate highlights the formidable obstacles organisations face when attempting to establish effective data governance frameworks. Additionally, a survey on information governance found that while 74% of respondents had a formal, enterprise-wide governance strategy, only 20% considered their strategies to be highly effective (Curtiss, J., Saxena, S. and Seth, A., 2018). This discrepancy indicates that even when organisations have formal governance programs in place, many struggle to ensure these initiatives are operating at an optimal level. Similarly, more than 60% of insurance plans have formal data governance programs, but 50% of these new programs fail to deliver the intended outcomes (Amitech., 2022). The high rate of failure in data governance implementation across various industries emphasizes the pressing need for organisations to better understand and overcome the key obstacles that hinder the realization of the strategic potential of data governance.

The academic literature suggests that while data governance can yield significant benefits for organisations, there are substantial challenges and barriers to its implementation due to the

deeply ingrained nature of these obstacles within the organisational context (Prinzo, R., 2012). Nonetheless, scholarly studies have acknowledged the necessity of developing a dedicated data governance framework to address the challenges of dark data governance (Splunk., 2019), (McNulty, K., 2017), (Kim, W. et al., 2003), (Agrawal, S., 2019). The academic and practice-oriented literature indicates that the development and implementation of data and dark data governance frameworks can be inherently complex, as organisations may encounter various challenges that could impact their decision to adopt such initiatives (Marus, P., 2018), (Marsh, S., 2019), (Redman, C, T., 2018), (Rees, V, I., 2020). This section provides an in-depth analysis of the key challenges identified in the academic and practice-oriented literature on data governance and dark data governance. Accordingly, the analysis classifies the key challenges into 17 for data governance (Section 3.7.4.1) and 15 for dark data governance (Section 3.7.4.2), each with similar definitions and contextual factors. The discussion examines the various explanations and perspectives from different sources and deals with the challenges based on their underlying meanings and contexts. Consequently, decision-makers should carefully consider and address these challenges before implementing data and dark data governance initiatives, in order to mitigate the inherent complexity and enhance the prospects of successful implementation.

The forthcoming sections (3.7.4.1. and 3.7.4.2) will provide a summary of the analysis of the key challenges encountered in the implementation of data governance (Table 3.7) and dark data governance (Table 3.8).

3.7.4.1. Analysis of Key Challenges for Data Governance Implementation

The key challenges to effective data governance implementation are outlined in Table 3.7. These identified challenges offer a comprehensive and clear depiction of the critical areas that organisations must prioritize to achieve successful data governance execution (details in Appendix C). Each thematic cluster encompasses related obstacles, facilitating a more strategic approach to addressing the complexities of managing data across modern enterprises. This thematic framework also underscores the interconnected nature of these challenges, emphasizing the necessity for holistic, adaptable, and continuously evolving governance frameworks.

ID	Challenge Name	Description
1	Standardization and Consistency	Lack of standardization in data governance practices leads to inconsistencies in data management across organisations and industries.
2	Data Quality Management	Ensuring high data quality across departments and throughout the data lifecycle remains a challenge, impacting governance effectiveness.
3	Organisational Culture and Resistance	Organisational resistance and cultural barriers, such as reluctance to share data, hinder the adoption of data governance initiatives.
4	Legal, Ethical, and Regulatory Compliance	Navigating evolving legal, ethical, and regulatory requirements, especially for global organisations, is a significant challenge for maintaining data governance compliance.
5	Accountability and Ownership	Unclear data ownership and fragmented accountability complicate governance structures, especially in collaborative environments.
6	Resource Allocation and Constraints	Limited budgets and skilled personnel, along with difficulty measuring ROI, hinder the effective implementation of data governance.
7	Technological Changes and Integration	Rapid technological advancements and the integration of legacy systems into modern data governance frameworks present ongoing challenges.
8	Complexity of Data Environments	Managing dynamic, complex data environments, including integrating structured and unstructured data, is increasingly difficult.
9	Data Security and Risk Management	Balancing data accessibility with security, particularly in the face of internal and external threats, is a critical challenge.
10	Cross-Departmental Coordination and Collaboration	Ensuring seamless collaboration and coordination across departments with differing priorities and practices is essential for successful data governance.
11	Governance in Dynamic and Agile Environments	Adapting data governance frameworks to dynamic, fast-paced environments, such as agile settings, is challenging due to conflicting needs for flexibility and structure.
12	Mergers, Acquisitions, and	Mergers, acquisitions, and multi-cloud strategies introduce complexities in aligning disparate systems and governance practices.

ID	Challenge Name	Description
	Multi-Cloud Strategies	
13	Data Lifecycle Management	Managing data throughout its entire lifecycle, from creation to deletion, remains a challenge, especially with the retention of unnecessary data.
14	Integration with Business Objectives	Aligning data governance frameworks with core business processes and strategic objectives is essential but difficult to achieve.
15	Data Governance in Specialized Data Environments	Governing data in specialized environments such as big data, IoT, and AI presents unique challenges, requiring governance models tailored to these contexts.
16	Real-Time Data Governance	Traditional governance models struggle to keep pace with real-time data processing, requiring adaptation for real-time analytics.
17	Continuous Improvement and Adaptation	Balancing innovation and control, ensuring stakeholder buy-in, and continuously evolving governance practices to meet technological and business demands are ongoing challenges in data governance.

Table 3. 7 Key Challenges for Data Governance Implementation

3.7.4.2. Analysis of Key Challenges for Dark Data Governance Implementation

Table 3.8 presents an overview of the key challenges that organisations must prioritize to enable effective implementation of dark data governance (details in Appendix D). This structured approach facilitates a deeper understanding of the complex landscape of dark data governance. Each thematic category encompasses related challenges, enabling a strategic focus on the areas demanding the most attention in dark data governance. This thematic structure also underscores the necessity for continuous improvement, adaptability, and strong alignment with organisational goals and processes to effectively manage and leverage dark data within the enterprise.

ID	Challenge Name	Description
1	Identification, Classification, and Retrieval of Dark Data	Identifying, classifying, and retrieving dark data is challenging due to its hidden nature and lack of visibility across systems.

ID	Challenge Name	Description
2	Data Security, Privacy, and Ethical Concerns	Managing dark data poses security, privacy, and ethical risks, especially when sensitive data is involved, often collected without clear consent or under outdated regulations.
3	High Costs and Resource Constraints	The costs of storing, processing, and analysing dark data are high, and organisations often struggle with resource constraints in managing these hidden data assets.
4	Integration and Interoperability Challenges	Integrating dark data with existing governance frameworks and mainstream data is difficult due to its unstructured nature and outdated formats.
5	Tools, Technology, and Automation	Inadequate tools for analysing and automating governance processes for dark data limit organisations' ability to manage these assets effectively.
6	Data Quality, Redundancy, and Cleansing	Dark data often contains duplicates or decayed information, complicating cleansing efforts and adding to storage costs.
7	Legal and Ethical Compliance Risks	Dark data can expose organisations to unforeseen legal and ethical risks, particularly in terms of compliance, data retention, and sensitive information handling.
8	Adaptability, Agility, and Change Management	The evolving nature of dark data requires organisations to be agile and adaptive in their governance practices to keep pace with new challenges and opportunities.
9	Data Categorization and Metadata Management	The lack of metadata and difficulty in categorizing unstructured dark data complicates efforts to manage and govern it effectively.
10	Coordination and Common Knowledge	Fragmented data sources, lack of awareness, and unclear accountability lead to challenges in governing dark data and increasing associated risks.
11	Supporting Business Processes and Goals	The uncertain value of dark data makes it difficult to justify governance investments, while mismanagement can result in security breaches and hinder business process support.
12	Corporate Policies and Data Architecture	Governing dark data within legacy systems and non-traditional formats complicates the creation of unified corporate policies and common data architecture.

ID	Challenge Name	Description
13	Data Integration and Interoperability	Ensuring interoperability of dark data across systems and addressing issues like data deletion complicates governance efforts.
14	Extracting Value from Data	Extracting actionable insights from unstructured dark data is challenging, with a high risk of misinterpretation and difficulty determining its relevance.
15	Continuous Improvement and Learning	Continuous adaptation and learning are required to manage dark data effectively as new technologies and data types emerge.

Table 3. 8 Key Challenges for Dark Data Governance Implementation

3.7.5. Analysis of Critical Success Factors

The critical success factor approach has gained prominence among researchers and is now widely employed as a powerful tool to aid strategic planning (Amberg, M., Fischl, F. and Wiener, M., 2005) and identify organisations' key information requirements (Forster, N. and Rockart, J., 1989). Additionally, the CSF framework exerts a substantial influence on the design, development, and implementation of data and information management initiatives within enterprises (Williams, J. and Ramaprasad, A., 1996). The CSF method enables organisations to systematically identify and focus on the most critical factors that are essential for the successful execution of their data-related projects and programs.

Literature presents various definitions of critical success factors. One common definition describes CSFs as the key areas of activity that require constant and attentive management oversight (Forster, N. and Rockart, J., 1989). Another definition characterizes CSFs as factors which, if properly addressed, can significantly enhance the likelihood of successful project implementation (Müller, R. and Jugdev, K., 2012). The purpose of the critical success factor approach is to systematically identify the key factors that managers deem essential for achieving their goals. Once these critical factors are determined, they are explicitly stated as part of the organisation's objectives, and the necessary information to monitor their performance is then identified (Forster, N. and Rockart, J., 1989).

Therefore, the complexity of dark data governance means that success in its implementation requires reference to a solid methodical foundation and proven scientific theories. It seems that the concept of CSFs provides a good basis for stating what criteria should be followed during the implementation of a dark data governance model. The complexity of dark data governance

necessitates a rigorous and systematic approach grounded in established methodological frameworks and validated scientific theories. The concept of critical success factors appears to provide a suitable foundation for outlining the key criteria that should guide the implementation of a dark data governance model (Amberg, M., Fischl, F. and Wiener, M., 2005). With regard to dark data governance, the CSFs refer to the important factors that are considered to be critical for the implementation of the dark data governance model. The results of the systematic review of data governance show that in the literature many authors have published a list of CSFs in relation to the implementation of data governance in organisations. Thus, to extract the common CSFs for implementing dark data governance, the study analyses and classifies the different factors related to data governance in general (Section 3.7.5.1) and dark data governance in particular (Section 3.7.5.2) that have been discussed in the literature review. These have therefore been consolidated into eleven main factors, each of which has similar definitions (Section 3.7.5.3). Under each main factor, there are sub-factors or different explanations from different resources. In addition, some of the factors have been mentioned in the same expression but in different meanings or contexts. Consequently, they have been dealt with based on their meanings or contexts. A consolidation of the most common CSFs that are important for implementing data governance and dark data governance, as reported in the literature, is presented in section 3.7.5.3 below. These CSFs are considered the key factors deemed essential for the successful implementation of a comprehensive dark data governance framework within organisations

3.7.5.1. Analysis of Critical Success Factors (CSFs) for Data Governance Implementation

The following structured critical success factors for data governance (Table 3.9) are focused on supporting key business operations and enabling the achievement of organisational goals (details in Appendix E). These CSFs provide a foundational basis for the successful implementation of comprehensive data governance programs within organisations.

ID	CSF	Description
1	Clear Data Governance Purpose to Support Business Processes and Objectives	Establish a comprehensive data governance framework aligned with business strategy and a clear vision to ensure data governance supports organisational objectives.

ID	CSF	Description
2	Clarity on Business Scope and Data Scope	Appoint data stewards, manage data lifecycle, and maintain a comprehensive data inventory to ensure alignment of data governance with business scope.
3	Business Compliance with Data Governance	Ensure adherence to regulatory compliance, privacy management, and legal standards to protect the organisation and maintain data governance integrity.
4	Coordination and Harmonization	Foster stakeholder engagement, cross-functional collaboration, and establish a governance committee to promote clear communication and alignment of governance initiatives.
5	Corporate Control and Cohesion	Implement robust access controls, clarify data ownership, and allocate resources to ensure consistent and accountable data governance across the organisation.
6	Corporate Policies for Key Data Governance Domains	Develop policies for data quality, retention, usage, and master data management, ensuring consistency, compliance, and ethical data use across the organisation.
7	Audit and Compliance Monitoring	Regularly monitor and audit data governance practices to ensure they meet regulatory and organisational standards, including third-party vendor compliance.
8	Adaptation and Intelligence	Implement agile governance practices to quickly adapt to external changes, adopt industry best practices, and proactively manage data governance risks.
9	Integrated Governance	Align data governance with IT governance, cloud environments, and enterprise architecture to ensure data integration, interoperability, and secure governance in various contexts.
10	Learning and Change Management	Manage changes effectively by preparing stakeholders through training, fostering adaptability in governance practices, and ensuring leadership involvement.
11	Governance Common Knowledge	Standardize data definitions and improve metadata management to maintain data quality and provide clarity for all stakeholders in governance activities.
12	Continuous Improvements for Data Governance	Establish continuous monitoring, KPIs, and maturity assessments for data governance to ensure ongoing improvement, adaptability, and alignment with long-term organisational goals.

Table 3. 9 Critical Success Factors (CSFs) for Data Governance Implementation

3.7.5.2 Analysis of Critical Success Factors (CSFs) for Dark Data Governance Implementation

The following critical success factors for dark data governance (Table 3.10) are focused on supporting key business operations and enabling the achievement of organisational goals (details in Appendix F). These CSFs provide a foundational framework for the successful implementation of comprehensive dark data governance programs within organisations.

ID	CSF	Description
1	Dark Data Governance Purpose to Support Business Processes and Goals	Align dark data governance with business strategy to drive value creation, support business goals, and leverage dark data for competitive advantage.
2	Business Scope, Data Scope, and Dark Data Classifications	Identify and classify dark data sources to prioritize management efforts based on data sensitivity, value, and relevance to the business.
3	Business Operations Compliance with Dark Data Governance Functions	Ensure compliance with data protection laws, conduct regular audits, and address privacy and legal risks associated with dark data.
4	Coordination and Harmonization	Promote cross-departmental collaboration, establish cross-functional dark data governance teams, and integrate dark data governance into existing frameworks.
5	Control, Cohesion, and Corporate Policies Development	Develop dark data governance policies, frameworks, roles, automate governance processes, and ensure data security and quality control.
6	Audit and Compliance Monitoring	Establish audit trails, review policies regularly, and track governance effectiveness using metrics and KPIs to ensure compliance and continuous improvement.
7	Adaptation and Intelligence	Align dark data governance with organisational goals, assess risks, and develop long-term strategies for managing dark data to maintain agility and adaptability.
8	Integrated Governance	Integrate dark data governance with corporate strategy, IT infrastructure, and cloud environments to ensure consistency and maximize value from big data analytics.
9	Corporate Learning and Change Management	Implement change management, regular training, and awareness programs to ensure employees are informed and engaged in dark data governance practices.

ID	CSF	Description
10	Continuous Improvements for Dark Data Governance	Continuously monitor dark data, define KPIs, and improve governance practices to ensure effective management and extraction of valuable insights over time.

Table 3. 10 Critical Success Factors (CSFs) for Dark Data Governance Implementation

3.7.5.3 Dark Data Governance CSFs: Consolidated Critical Success Factors (CSFs) for Data Governance and Dark Data Governance Implementation

The comprehensive consolidation presented in Table 3.11 covers all critical success factors across both data governance and dark data governance, ensuring that each key theme is thoroughly addressed and seamlessly integrated into a cohesive and highly effective governance strategy (details in Appendix G). By concentrating on these critical success factors, organisations can develop comprehensive and resilient governance frameworks that are closely aligned with their strategic goals, capable of adapting to evolving environmental and operational circumstances, and positioned to extract optimal value from all data assets while effectively managing dark data within the organisational context. Implementing a robust data governance program anchored in these key factors can enable enterprises to harness the full potential of their data resources, including dark data, in support of their overarching business objectives. This approach helps organisations establish a strong, sustainable data management foundation while counteracting dark data that is responsive to changing needs and empowers data-driven decision-making and innovation across the organisation.

Table 3.11 and Figure 3.15 presented below in this section provide a clear and well-structured summary of the critical success factors for implementing an effective dark data governance framework within organisations.

CSF	Description
CSF1: Strategic Alignment and Purpose	Ensures data governance and dark data governance are aligned with the organisation's business strategy, integrating frameworks, leveraging data for business intelligence, innovation, and supporting long-term business goals.
CSF2: Business Scope, Data Scope, and Dark Data Classifications	Focuses on data stewardship, lifecycle management, classification standards, and comprehensive data inventories to manage data effectively within the defined scope. Identifies and classifies dark data sources.

CSF	Description
CSF3: Business Operations Compliance with Governance Policies, Standards, and Regulations	Ensures adherence to regulatory requirements, privacy management, develops best practices, addresses legal/ethical considerations for dark data, and establishes retention, disposal, and corporate policies.
CSF4: Coordination, Collaboration, and Communication	Involves active stakeholder engagement, cross-functional collaboration, establishing governance committees, ensuring communication strategies, and engaging with regulatory bodies for both data and dark data governance.
CSF5: Corporate Control, Cohesion, and Corporate Policy Development	Focuses on data access controls, defining corporate roles, incident management, corporate policy development, data quality control, metadata management, and resource allocation to ensure cohesion across the organisation.
CSF6: Audit and Monitoring	Regularly monitors and audits data governance processes, conducts data protection impact assessments, ensures auditable processes, including third-party governance, and tracks dark data governance metrics and KPIs for improvement.
CSF7: Adaptation, Agility, and Learning	Adapts to environmental changes, adopts best practices, implements agile governance, develops long-term strategies for data governance, manages risks proactively, and aligns with organisational strategic goals.
CSF8: Integrated Governance	Aligns data governance with Corporate governance, IT governance, integrates governance in cloud environments, enterprise architecture, and big data analytics, ensuring dark data governance is integrated into existing frameworks and supports business goals.
CSF9: Corporate Metadata Management and Common Understanding	Manages metadata effectively, establishes standardized data definitions, fosters a shared understanding across the organisation, ensuring consistency and reducing misinterpretation for common understanding.
CSF10: Training and Change Management	Manages changes in governance practices, provides training for stakeholders, promotes dark data awareness, ensures transparency, and builds a culture of understanding and protecting data and dark data across the organisation.
CSF11: Continuous Improvements and Maturity Models	Establishes continuous improvement processes, defines and tracks KPIs, regularly assesses governance maturity, and ensures ongoing evaluation to keep governance practices relevant and effective.

Table 3. 11 Dark Data Governance CSFs

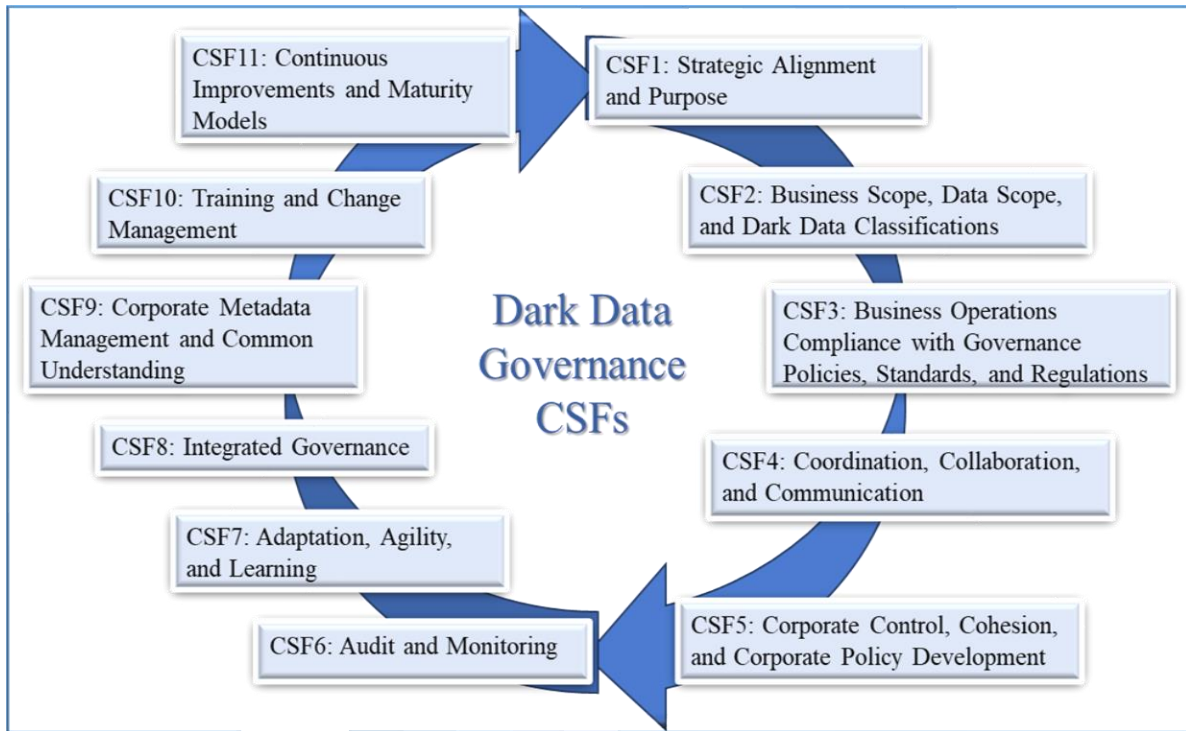


Figure 3. 15 Dark Data Governance CSFs

3.8 Critical Review Findings

The critical review of existing literature on data governance and dark data governance reveals significant gaps in addressing a holistic context. Current frameworks often focus on isolated aspects of governance—such as technological solutions, compliance, or specific organisational functions—without considering the broader organisational and strategic context. This fragmented approach leads to several key issues. Firstly, many frameworks fail to integrate data governance across all organisational functions, resulting in silos that hinder effective data management and strategic alignment. For instance, Abraham, Schneider, and Brocke (2019) highlight that most data governance models lack comprehensive integration, which prevents organisations from fully leveraging their data assets across different departments. Similarly, Al-Ruithe, Benkhelifa, and Hameed (2018) discuss the technological disparities between cloud and non-cloud environments, noting that current governance frameworks do not effectively bridge these gaps, leading to inconsistencies and inefficiencies in data management. Moreover, ethical considerations and human factors are frequently overlooked in existing data governance models. Alreemy et al. (2016) identify critical success factors for information technology governance but note that many frameworks fail to incorporate ethical considerations, such as data privacy and security, into their governance structures. This omission can result in ethical dilemmas and legal risks, as highlighted by Thiel, Stroetmann, and Singleton (2014), who

emphasize the need for ethical guidelines in clinical data governance. The management of dark data is another area where a holistic context is often missing. Dark data, especially the vast amount of data that is collected but not used, poses significant risks and opportunities for organisations.

However, many data governance frameworks treat dark data as an afterthought, if at all. Judah and White (2021) point out that most governance models do not adequately address the management of dark data, leading to underutilization and potential risks associated with unmanaged data. Effective data governance requires skilled personnel who understand both the technical and strategic aspects of data management. Niemi and Laine (2016) discuss how many governance frameworks fail to address the need for competence management, leading to a gap between the governance policies in place and the actual ability of staff to implement them effectively. This disconnect can result in poor execution of governance strategies and a failure to achieve desired outcomes. Furthermore, the focus on technological solutions in dark data governance often comes at the expense of socio-technical integration. Cheng et al. (2017) propose a maturity model for cloud data governance that is heavily centred on technology but neglects the human and organisational factors that are crucial for comprehensive governance. This technological-centric approach fails to account for the complexities of managing dark data in a way that aligns with broader organisational goals and ethical considerations.

The evidence presented highlights the need for a more holistic approach to data governance, particularly when managing dark data. This is crucial for the following key reasons:

- **Unified Strategy Across Organisational Functions:** A holistic governance framework ensures that data management practices are unified and consistent across all organisational functions. This consistency is essential for achieving strategic alignment, as it ensures that all departments are working towards the same goals and using data in a way that supports the organisation's objectives (Abraham, Schneider, and Brocke, 2019; Weber, Otto, and Osterle, 2009). Without this integration, data governance efforts can become fragmented, leading to inefficiencies, duplicated efforts, and conflicting strategies that undermine organisational effectiveness (Gimpel, 2020; Otto, 2011).
- **Enhanced Decision-Making and Innovation:** Dark data, when effectively managed, can provide insights that drive better decision-making and foster innovation. A holistic approach to data governance ensures that dark data is not overlooked but rather integrated with other data sources to create a more holistic and accurate picture for decision-makers (Lavalle and Smilde, 2021; McNulty, 2017). This comprehensive data management allows

organisations to identify new opportunities, optimize processes, and develop innovative solutions that might otherwise remain hidden in ungoverned data (Trajanov et al., 2018).

- **Compliance and Ethical Considerations:** Dark data often contains sensitive information that, if not properly managed, can lead to significant compliance and ethical issues. A holistic governance framework ensures that all data, including dark data, is handled in compliance with relevant regulations and in accordance with ethical standards (Thiel, Stroetmann, and Singleton, 2014; Hand, 2020). This comprehensive approach not only protects the organisation from legal risks but also enhances its reputation by demonstrating a commitment to responsible data management (Johnson, 2020; Deloitte, 2017).
- **Optimizing Resource Allocation:** Effective dark data governance through a holistic framework ensures that resources are allocated efficiently. Organisations can avoid wasting resources on collecting and storing data that is never used or analysed (Smallwood, 2012; Gimpel, 2020). Instead, a holistic approach prioritizes the management of valuable data, ensuring that resources are focused on data that can provide strategic value. This optimized resource allocation helps organisations reduce costs and improve the return on their data investments (McNulty, 2017).
- **Improved Risk Management:** Dark data presents significant risks, including the potential for data breaches, non-compliance with regulations, and the loss of critical information. A holistic governance framework ensures that these risks are identified, assessed, and managed proactively (Sun, Su, and Shen, 2023; Judah and White, 2021). By integrating dark data into the broader governance strategy, organisations can implement controls and safeguards that mitigate these risks, thereby protecting their data assets and ensuring business continuity (Deloitte, 2017; Marsh, 2019).
- **Adaptability in a Dynamic Technological Landscape:** The rapid pace of technological change, particularly with the advent of big data, IoT, and Artificial Intelligence (AI) tools, requires governance frameworks that are adaptable and flexible. A holistic approach ensures that data governance can evolve to meet new challenges, such as the integration of dark data from diverse and emerging sources (Cheng et al., 2017; Trajanov et al., 2018). This adaptability is crucial for maintaining effective data governance in a world where technology and data sources are constantly changing (Gimpel, 2020).
- **Addressing the Full Data Lifecycle:** Dark data often emerges because of inadequacies in lifecycle management, where data is collected and stored but not actively used. A holistic governance framework addresses the full data lifecycle—from collection and storage to analysis and eventual disposal—ensuring that all data is managed effectively throughout

its life (Redman, 2016; Côte-Real, Ruivo, and Oliveira, 2020). This comprehensive management reduces the likelihood of data becoming "dark" and ensures that all data assets are utilized to their fullest potential (Wiebe and Allison, 2015).

- **Leveraging Dark Data for Competitive Advantage:** Dark data, when effectively governed, can provide a competitive advantage by uncovering insights that competitors may overlook. A holistic approach to data governance ensures that dark data is systematically analysed and integrated with other data, enabling organisations to gain unique insights into market trends, customer behaviour, and operational efficiencies (Gimpel, 2020; McNulty, 2017). This strategic use of dark data can lead to innovative products, services, and strategies that differentiate an organisation in the marketplace (Trajanov et al., 2018).

In summary, a holistic perspective in data governance, particularly for dark data governance, is not merely advantageous but fundamental. It ensures that data governance practices are cohesive, inclusive, and aligned with the organisation's overarching strategic goals. By embracing a holistic approach, organisations can optimize the value of their data assets, mitigate risks, uphold compliance, and cultivate innovation, ultimately culminating in enhanced organisational performance and competitive edge. Organisations that lack a holistic data governance approach are vulnerable to inefficiencies, risks, and missed opportunities, which highlights the critical need for a comprehensive governance framework in the modern data-driven landscape.

3.9 Chapter Summary

This chapter focuses on a comprehensive literature review of data governance and dark data governance, emphasizing their critical roles in organisational management. The review underscores the growing importance of effectively managing data assets, driven by advancements in big data and the increasing complexity of data and information management. It advocates for a holistic approach to data governance, which integrates data as a strategic asset across organisational boundaries and aligns data management practices with broader corporate governance structures. Furthermore, the chapter highlights the evolution of data governance from a narrower focus on data quality and regulatory compliance to a more comprehensive approach encompassing data privacy, information security, and strategic decision-making. The review adopts a rigorous tertiary review methodology, examining existing research on data governance and dark data governance to identify frameworks,

challenges, and critical success factors. The analysis reveals a significant shift towards recognizing the importance of dark data governance, driven by the realization of the potential value hidden in unutilized data. The chapter identifies a research gap in the implementation of holistic data governance for dark data and provides a critique of the relevant literature followed by a summary that includes the identification of gaps. Ultimately, the chapter advocates for the integration of data governance into broader organisational strategies to unlock the full potential of data, particularly dark data, which poses unique challenges and opportunities. The findings suggest that holistic dark data governance is crucial for fostering innovation, operational efficiency, and regulatory compliance, making it an essential component of modern organisational management.

The following chapter will present a proposed holistic framework to design, deploy, and sustain a viable dark data governance model.

Chapter 4. A Holistic Framework for Dark Data Governance

4.1. Introduction

Based on our previous discussion, it is evident that there are currently no comprehensive frameworks for data governance that effectively address dark data issues within an organisational holistic context. Existing frameworks have primarily focused on data governance structure, data quality, and the necessary processes for implementing data governance with key components. However, such frameworks have been presented without consideration for dynamic alignment with business objectives, and interconnectedness between governance components and the broader holistic ecosystem for organisations. Examples of these frameworks were discussed in Chapter 3. Therefore, our main aim in this chapter is to propose a holistic framework for dark data governance that addresses these limitations

The proposed holistic framework for dark data governance aims to address the limitations of existing frameworks by considering dynamic alignment with business objectives and interconnectedness between governance components and the broader ecosystem of the organisation ([Wibowo, S. N., Utami, E. and Fatta, A. H., 2021](#)). This framework recognizes the strategic importance of data governance in today's digital era and emphasizes the need for alignment between data, technology, and business objectives. It also acknowledges the organisational changes and mindset shift required for successful data governance implementation.

Data governance is not a destination nor a project, but a system as a continuous journey and functions that need to be measured and sustained, so that it becomes a vital process with goals which are continuously revised to improve data and support the changes in business goals. As such, successful data governance adoption in the cultural fabric of the organisation requires a combination of several contributing systemic elements especially human factors and technology ([Mahanti, R., 2021](#)) within a system context.

Since Dark Data governance places significant emphasis on mitigating and overseeing risks associated with dark data to assist companies in achieving their aims and targets, this research views dark data governance as a subset of the broader governance framework within the overall context of cybernetics, the Viable System Model (VSM) and systems thinking theories. In this thesis, a holistic novel model for governance in general and specifically for dark data governance is introduced as part of the presented work. This chapter thus outlines the proposed framework aimed at establishing and maintaining a viable holistic dark data governance model.

The proposed framework for dark data governance aims to establish and maintain a viable holistic model that effectively governs and counteracts dark data ([Dunsin, D. et al., 2023](#)).

The framework is developed based on the viable system model (VSM) theories and critical success factors (CSFs) concept. As part of the framework development in this chapter, the dark data and data governance taxonomies are extracted from the literature to understand the key dimensions involved in dark data governance. Based on this information, the dark data governance key dimensions are presented as part of the holistic data governance framework development. The framework proposed in this chapter takes into account the interconnectedness between governance components and the broader ecosystem, while also aligning with business objectives ([Yuan, F., Meng, J. and Li, Y., 2020](#)). Also, it recognizes the need for effective collaboration and training across organisational boundaries ([Wibowo, S, N., Utami, E. and Fatta, A. H., 2021](#)). The framework emphasizes the importance of data governance in addressing dark data risks and highlights the need for organisational changes and a data-oriented mindset ([Jones, K. et al., 2020](#)). This framework aims to provide organisations with dynamic systemic components within a holistic system to effectively govern and counteract dark data, resulting in improved decision-making, enhanced operational viability, and stability.

This chapter describes the systemic components of the framework and how the different components of the framework interact with each other. The different components' activities of the framework are discussed, and a justification is given for why these components are crucial to ensure the stability of the organisation. Additionally, guidelines on how to manage the framework implementation are also presented in this chapter. This study shows how the secondary research has informed the development of the framework, and an overall summary of the framework is presented.

4.2. Theoretical Foundation

This section offers insight into the theoretical foundation of the research. A theoretical basis guides the researcher in interpreting study results ([Simon, M. and Goes, J., 2011](#)). Academic researchers and practitioners agree that the lack of data governance has various impacts on organisational strategies and their ability to achieve their mission and goals. Both sides share the consensus view that data governance is not a one-size-fits-all proposition ([Weber, K., Otto, B. and Osterle, H., 2009](#)). However, to the best of the author's knowledge, there are no

empirical studies in academic literature that address holistic viable data governance for dark data.

This research aims to close this gap by developing a holistic framework to understand how to implement a data governance system for counteracting dark data based on a comprehensive analysis of data governance in both science and practice. In the following section, the author will consider various theories and concepts from the literature to establish the theoretical foundation of this research. This will be the basis for constructing the study's conceptual holistic framework. These theories and concepts are the following:

4.2.1. Critical Success Factors (CSFs) Concept

In combination with the viable system model theories (section 4.2.2), critical success factors (CSFs) defined in Chapter 3 (section 3.7.5) are employed in the development of the holistic framework for dark data governance. These factors provide a unique holistic context to the framework development that is not addressed within existing models. Consequently, this chapter will consider the CSFs pertinent to the implementation of data governance in general and in particular for mitigating dark data. The theoretical foundation provided by the CSF concept is robust and supports this objective effectively. Over the past three decades, the concept of CSFs has been extensively researched, particularly initiated by Rockart in 1979 ([Forster, N. and Rockart, J., 1989](#)). This approach is increasingly utilised to support information systems (IS) strategic planning by consultants and IS departments ([Amberg, M., Fischl, F. and Wiener, M., 2005](#)).

The majority of research within the critical success factor domain has been theoretical, often adopting a static view of the significance of various factors throughout the life cycle of a project ([Pinto, K. J. and Prescott, E. J., 1988](#)). The literature indicates that the CSF concept is crucial for achieving overall organisational objectives, missions, and strategies. It is appropriate for both individual business units and the overarching organisational goals, aligning with the fulfilment of the organisation's objectives ([Amberg, M., Fischl, F. and Wiener, M., 2005](#)). Clearly establishing CSFs is a vital component of dark data risk management and is essential for the successful implementation of data governance ([Ladley, J., 2012](#)). The process of CSF identification, validation, and analysis of underlying constraints, followed by the determination of necessary measures for each identified CSF, is repetitive and ongoing ([Amberg, M., Fischl, F. and Wiener, M., 2005](#)). Therefore, the successful governance of dark data necessitates the identification and management of multiple CSFs.

4.2.2. The Viable System Model (VSM) Theories – based on Cybernetics and Systems Theories

This research seeks to fill the existing limitations and challenges discussed in Chapter 3 and provides a systemic approach to managing dark data risks, ultimately contributing to unlocking the untapped potential of organisational data and maximizing its business value to achieve required goals. To develop a comprehensive understanding of data governance for dark data, the researcher will consider various approaches and concepts from the literature ([Dunsin, D. et al., 2023](#)). As data becomes increasingly integral to business models where digital transformation and artificial intelligence continue to reshape industries, the governance of dark data emerges as a critical area of focus. Dark data refers to the vast amount of data that organisations collect but are not effectively used or analysed ([Jones, K. et al., 2020](#)) to achieve set goals.

In Chapter 3, as previously discussed, the absence of a holistic approach to organizing data governance and information technology governance may pose challenges for organisations in uncertain eco-system-based environments, making them less viable against rapidly changing threats related mainly to dark data. Viability is defined as the capability of an organisation to continue to strive to accomplish its goals within its complex ecosystem ([Beer, S., 1979](#)). Managing and governing this complexity can only be done by looking at the organisation from a holistic context. A cybernetics and systems thinking approach will be applied to this research, as cybernetics and systems thinking approaches imply holism by design([Espejo, R. and Gill, A., 2011](#)), ([Andrew, A., 2007](#)),([Beer, S., 1979](#)). Cybernetics and systemic thinking advocate a holistic view on the whole system as a set of elements and the analysis of the relationships between these elements ([Preece, G., Shaw, D. and Hayashi, H., 2013](#)), as these may lead to emergent properties that are even more important than the individual elements themselves([Espejo, R. and Reyes, A., 2011](#)). Both terms cybernetics and governance are derived from the Greek *kybernetike*, which stands for” the art of steersmanship” ([Schwaninger, M., 2018](#)). In modern times, the governor has been used for management systems ([Beer, S., 1967](#)). From a cybernetic view, there is little difference between governance on the one hand, and management or control, on the other. In organisations, the principles of governance have evolved over time and the approaches to governance have had to change from a reductionist way of looking at things to systemic viability. Systemic viability focuses on the capacity of an organisation to maintain and develop its core functions amidst changing external conditions. It involves creating governance structures that are flexible, adaptive, and capable of learning and evolving in response to internal and external pressures ([Espejo, R. and Reyes, A., 2011](#)).

Several systemic methodologies to study (complex) systems were discussed ([Flood, L. R. and Jackson, C. M., 1991](#)), one of the methodologies that view organisations as a viable complex system is the VSM ([Beer, S., 1981](#)). VSM emphasizes active learning and control and is therefore particularly useful for systems that are operating in highly uncertain environments. Systemic methodologies generally rely heavily on visual representation. VSM is the visual representation of the viable system view ([Beer, S., 1979](#)), ([Beer, S., 1972](#)), ([Beer, S., 1985](#)), ([Beer, S., 1981](#)). The VSM is theoretically grounded in systems theory and cybernetics where cybernetic principles were applied to the management of organisations “management cybernetics” ([Beer, S., 1959](#)), and effectiveness of organisations “cybernetics is the science of effective organisation” ([Beer, S., 1985](#)). As such VSM can be considered as “a theory of organisation” ([Anderton, R., 1989](#)). Stafford Beer is considered to be the first to translate cybernetic principles to the field of management and governance, ultimately resulting in the VSM ([Beer, S., 1959](#)), ([Mingers, J. and White, L., 2010](#)). Beer’s motivation is based on the fact that cybernetics embrace viability that reflects the capability of an organisation (as a complex system) to maintain itself in a changing environment ([Shaw, R. D. et al., 2004](#)) - contrary to the traditional ways of thinking about the management and governance of organisations that do not embrace the key concept of viability ([Beer, S., 1985](#)). Cybernetics is defined as “the science that studies the abstract principles of organisation in complex systems. It is concerned not so much with what systems consist of, but how they function. Cybernetics focuses on how systems use information, models, and control actions to steer toward and maintain their goals while counteracting various disturbances” ([Heylighen, F. and Joslyn, C., 2003](#)). Cybernetics is of a Greek origin, meaning “Steersman” ([Wiener, N., 1948](#)). The VSM provides a theoretical framework for understanding the functioning and effectiveness of organisations ([Kim, H. D., 2024](#)).

This study will follow the VSM theories as a Theoretical framework. The viable system view can be classified as a ‘functionalist’ system thinking approach, for which the underpinning is that “systems appear as objective aspects of a reality independent of us as observers”. This means that the systems are treated as real world ontological entities ([Reynolds, M. and Holwell, S., 2010](#)). However, it is entirely possible to take a more ‘interpretivist’ position with the VSM ([Preece, G., Shaw, D. and Hayashi, H., 2013](#)), where the underpinning is that “multiple perceptions of reality exist, and sometimes come into conflict”. In this view, systems are treated as epistemological constructs rather than ontological entities ([Reynolds, M. and Holwell, S., 2010](#)). When using the VSM as a lens to describe qualitatively, diagnose, or design data

governance, a more interpretivist position is taken([Zolfagharian, M. et al., 2019](#)). As such, this study will follow an Interpretive paradigm philosophy.

Empirical studies into the governance of data have advanced our understanding of the mechanisms used to control the use of data management. However, there has been relatively little research into the formulation of a theoretical model of governance that explains and organises the growing collection of parts into a coherent whole. To further advance the concept of data governance, VSM is proposed as a viable holistic governance model. Given that governance and cybernetics are both concerned with the control of sociotechnical systems, and Stafford Beer formulated the VSM as a blueprint for designing the control and communication (information) aspects of organisations ([Beer, S., 1972](#)). As such, VSM establishes a firm theoretical foundation upon which to formulate a model for governing the data governance function. This is due to the novel aspects of the VSM that will enable seamless integration of corporate governance, data governance and IT governance (even data management) at intra- and inter-organisational levels where the past and future meets under a single cohesive and adaptable holistic context.

The VSM view ([Beer, S., 1979](#)),([Beer, S., 1985](#)),([Beer, S., 1981](#)) uses systems and cybernetic thinking to enable detailed analysis of organisations. The approach enables modelling and diagnosis of threats (dark data in this study) to “viability.” Viability was defined by Beer (1979) to mean existence, but later interpretations (and the one adopted in this study) suggest that viability is more aligned with effectiveness([Preece, G., Shaw, D. and Hayashi, H., 2013](#)); ([Yolles, M., 2005](#)). VSM advocates that organisations will be viable if they perform a set of functions and manage information appropriately in those functions ([Achterbergh, J. and Vriens, D., 2002](#)); ([Schwaninger, M., 2006](#)). However, despite such claims, the literature highlights that VSM’s influence on the analysis of information has been relatively limited in the literature ([Paucar-Caceres, A. and Pagano, R., 2009](#)); ([Richter, J. and Basten, D., 2014](#)). Often cited criticisms of VSM is that it is too abstract for designing detailed information structures([Schwaninger, M. and Ríos, J., 2008](#)) and is generally too difficult to use ([Espejo, R., Bowling, D. and Hoverstadt, P., 1999](#))([Schwaninger, M. and Ríos, J., 2008](#)). These issues have hindered its widespread adoption but recently there have been further implementation guidelines to aid its use ([Hildbrand, S. and Bodhanya, S., 2015](#)).

In the context of this research, cybernetics and systems thinking approaches emphasize the importance of taking a holistic view of a system ([Kim, H. D., 2024](#)) within the viable system model (VSM) context. Therefore, by employing the VSM, it becomes possible to understand

and manage organisations as complex systems in a way that ensures their viability and adaptability in uncertain environments ([Ramírez–Vizcaya, S. and Froese, T., 2019](#)).

Based on the above concepts and theories, this study proposes the conceptualization of a Holistic Data Governance Model as a framework that addresses the specific challenges and risks of dark data, taking into consideration the critical success factors defined in Chapter 3 and the critical constructs for systemic viability within the VSM holistic context.

4.3 VSM as a Holistic Governance Framework for Organisations

This study proposes a dynamic way of looking at data governance and in particular dark data governance within the holistic ecosystem of an organisation based on VSM theories. The VSM provides a framework for designing flexible, adaptable organisations that balance external and internal perspectives and long and short-term thinking to gain a holistic cohesion while achieving the organisation's purpose. VSM describes organisations as a system regulating the processing of variety (data & information) ([Beer, S., 1979](#)),([Beer, S., 1985](#)),([Beer, S., 1981](#)).

In the VSM, organisations are not described in terms of people, jobs, positions, or corporate functions, but by the systemic functions that are necessary for the functioning and viability of the entire organisation. A viable organisation is an autonomous organisation that can survive by adapting to a changing environment and maintaining stability in its behaviour by virtue of its ability to maintain its operations.

The generality of the VSM makes it a powerful conceptual tool for both organisational diagnosis and design, independent of the specific features of the organisations under study, such as type of activity, size, location, products, markets, technology, and the like. Based on Systems and Cybernetics thinking, any organisation can be viewed as a viable system. In the sense of the VSM, viability means the ability of an organisation to organise itself, to meet the challenges of the environment, to act autonomously, and to choose its future itself. VSM has been used extensively as a conceptual tool ([Lassl, W., 2019](#)) for various organisational purposes:

- aids in understanding organisations, redesigning them when necessary, and supporting the management of change. Additionally,
- VSM facilitates both functional decentralization and the cohesion of the entire organisation. The VSM model is grounded in fundamental cybernetic principles of communication and control within complex organisations. These principles enable true autonomy and

empowerment within an integrated framework, while ensuring necessary links between individual parts.

- provides a framework for designing a flexible and adaptable organisation within an ecosystem. It achieves this by balancing long-term external perspectives with short-term internal needs, thereby fusing present requirements with future aspirations.

The VSM offers a way of gaining both functional decentralization and cohesion of the whole. It is underpinned by fundamental cybernetic principles of communication and control in complex organisations. These principles offer a way of providing true autonomy and empowerment within an integrated framework, together with the necessary supporting links between the individual parts. Key underlying concepts of the VSM is presented under section 4.3.1. below. Viability is considered as the key underlying concept of the VSM. It means that the system is able to continue achieving its purpose, despite being exposed to risks. Based on VSM, a viable organisation needs to have five key systems with balanced interactions ([Espejo, R. and Gill, A., 2011](#)), ([Yolles, M., 2006](#)), ([Beer, S., 1979](#)), ([Beer, S., 1985](#)). The five system functions (discussed in section 4.3.2.) are the necessary and sufficient concepts that enable viability. These system functions are interconnected through variety loops (discussed in section 4.3.3) to enable variety engineering (i.e., achieving requisite variety). The concept of recursion is also important in variety engineering (i.e., it enables variety engineering at different levels of granularity), and therefore, ultimately in achieving viability. In terms of variety engineering, transduction is concerned with variety preservation while translating the message into terms that the receiving entity understands. To summarize, the VSM can be considered as a dynamic model to support the diagnosis of effective control and communication structures ([Espejo, R. and Reyes, A., 2011](#)), thoroughly anchored in the theory of cybernetics.

The following describes the VSM key underlying concepts (section 4.3.1), VSM five systems (section 4.3.2), and key VSM variety loops (section 4.3.3), emphasizing the interconnectivity and adaptability necessary for systemic viability ([Huygh, T. and Haes, D, S., 2019](#)), ([Lowe, D., Espinosa, A. and Yearworth, M., 2020](#)). Section 4.3.4 describes the key VSM communication channels and section 4.3.5. describes the key VSM information flows.

4.3.1. VSM Underlying Concepts

4.3.1.1 Viability

A system is viable if it can maintain its identity ([Shaw, R, D. et al., 2004](#)) and continuously cope with the variety it faces ([Jackson, M., 1991](#)). Viability is closely related to the concept of

variety, which measures complexity. A viable system must have its own problem-solving capacity ([Espejo, R. and Harnden, R., 1989](#)) and quickly adapt to environmental changes at any given time by creating sufficient variety when detecting changes in the environment ([Pollalis, A, Y. and Dimitriou, K, N., 2008](#)).

4.3.1.2 Requisite Variety

Variety is a measure of complexity ([Beer, S., 1979](#)). To be viable, a system must cope with this variety. Ashby's law of requisite variety states that only variety can absorb variety, meaning the variety of the controlling element should be at least as great as that of the element being controlled. Variety engineering occurs at each communication channel of the VSM ([Ashby, R. W., 1956](#)).

4.3.1.3 Recursivity

The Viable System Model (VSM) is inherently recursive. Recursivity (Figure 4.1 – VSM Symbols are described in Appendix H) indicates that any viable system contains and is contained within another viable system ([Beer, S., 1979](#)). Each embedded viable system deals with its local environment, a subset of the total environment of the system-in-focus (level of recursion in focus). The VSM is fractal in nature, meaning that each viable system, at any given level of recursion, can be modelled using exactly the same syntax ([Espejo, R. and Harnden, R., 1989](#)). This enables consistent modelling at different levels of granularity. Also, Organisational goals within the recursive VSMs are typically recursive, where the higher-level viable system goals control the settings for the contained, lower-level viable system goals ([Heylighen, F. and Joslyn, C., 2003](#)).

4.3.1.4 Transduction

Transduction applies to the communication channels of the VSM. It implies that the communication between two entities should be translated into terms that the receiving entity understands, while preserving the intended variety ([Beer, S., 1985](#)).

4.3.2. VSM Five Systems

System1 (S1) – Operations/Implementation: S1 includes all systemic functions and activities that implement the system's purpose (operational units and primary activities) and managerial activities directly related to this (local management units). At any level of recursion, S1 consists

of all embedded viable systems with their goals and sub-goals, combining operational and local management units ([Heylighen, F. and Joslyn, C., 2003](#)), ([Beer, S., 1979](#)), ([Beer, S., 1985](#)).

System 2 (S2) – Harmonization/Co-ordination: S2 includes all systemic functions and activities that coordinate the activities of S1 (support activities). They represent an auto-regulation process to handle oscillations arising from interactions within or between embedded viable systems ([Beer, S., 1979](#)). S2 mechanisms can reflect managerial decisions but do not make them ([Beer, S., 1985](#)).

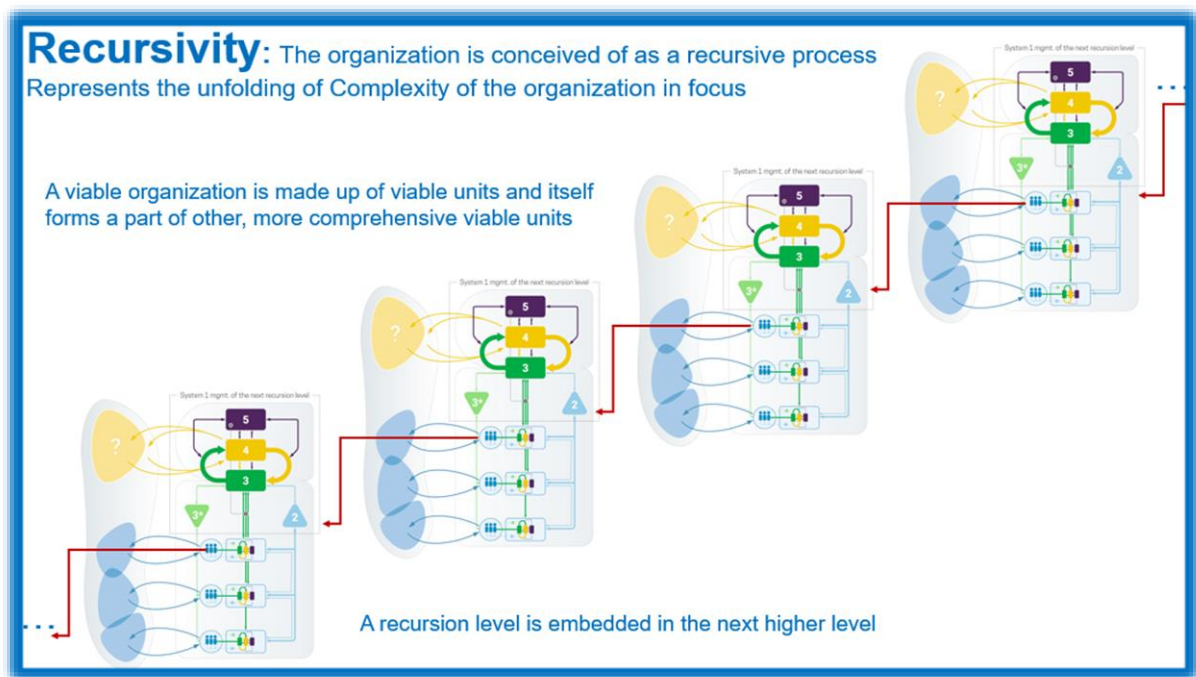


Figure 4. 1 Viable System Model (VSM) Recursivity

System 3 (S3) – Cohesion (Control and Autonomy): S3 includes all systemic functions and support activities to control the operation of S1 with its recursive viable systems and their embedded sub-goals ([Heylighen, F. and Joslyn, C., 2003](#)), ([Beer, S., 1985](#)). They balance the autonomy of all embedded viable systems with overall cohesion [160], focusing on the present management functions ([Reynolds, M. and Holwell, S., 2010](#)).

System 3* (S3*) - Audit and Compliance : S3* includes all audit systemic functions and support activities that enable S3 to obtain information directly from S1 operational units ([Beer, S., 1985](#)).

System 4 (S4) – Intelligence/Planning: S4 includes all systemic functions and support activities to sense opportunities and threats in the system's environment that could threaten its viability ([Espejo, R. and Harnden, R., 1989](#)). They manage potential future states of the system,

engage in external communication, and maintain a self-referential model of the system ([Beer, S., 1985](#)), ([Reynolds, M. and Holwell, S., 2010](#))([Reynolds, M. and Holwell, S., 2010](#)).

System 5 (S5) - Policy: S5 is the ultimate decision-making within a recursion of the viable system thereby providing logical closure to it ([Beer, S., 1985](#)), and creating and maintaining the system's identity ([Beer, S., 1979](#)). S5 includes all systemic functions and support activities to set the system's overall direction, values, and purpose, and monitor the feedback loop between current (S3) and future (S4) management systemic functions to ensure balance ([Beer, S., 1985](#)), ([Espejo, R. and Gill, A., 2011](#)), ([Reynolds, M. and Holwell, S., 2010](#)).

4.3.3. VSM Communication Key Variety Loops

4.3.3.1 Communication with the Environment - Variety Loop 1 (VL1): The system-in-focus communicates with its environment through S1 with its embedded viable systems and through S4 with the total environment. This communication involves both short-term and long-term activities focused on identifying and responding to current and anticipated opportunities and threats within the system's environment to achieve organisational goals ([Beer, S., 1979](#)), ([Beer, S., 1985](#)).

4.3.3.2 Inter-operational Management - Variety Loop 2 (VL2): includes communications among S1, S2, and S3 to manage operational complexity and enable effective decision-making through harmonization, self-regulation, and synergies ([Lowe, D., Espinosa, A. and Yearworth, M., 2020](#)).

4.3.3.3 S3 and S4 Homeostat (Monitored by S5) - Variety Loop 3 (VL3): The variety loop between S3 and SFs-4 balances the relationship between the present and the future, involving strategic decision-making ([Reynolds, M. and Holwell, S., 2010](#)). S5 monitors this loop to ensure alignment with the system's overall direction, values, and purpose ([Beer, S., 1985](#)), ([Espejo, R. and Gill, A., 2011](#)). It combines internal and external perspectives on feasible and desirable future developments, to support strategy development for the organisation ([Lowe, D., Espinosa, A. and Yearworth, M., 2020](#)).

4.3.3.4 Command Axis - Variety Loop 4 (VL4): The command axis, comprising S3, S4, and S5, provides the metasystem with decision-making capabilities. It balances present and future orientations and internal and external perspectives to maintain homeostasis. The command axis ([Beer, S., 1979](#)), ([Beer, S., 1985](#)), ([Reynolds, M. and Holwell, S., 2010](#)), ([Lowe, D., Espinosa, A. and Yearworth, M., 2020](#)) includes:

- The resource bargaining and accountability channel is a crucial component of the Viable System Model (VSM). The resource bargaining aspect encompasses the allocation of various resources, such as financial, human, knowledge-based, and time-related, to the operational units (S1). The more resources these units receive, the more capable and flexible they become in their actions. Conversely, a restriction of resources diminishes the scope and adaptability of the S1 units. However, the resource allocation channel alone is not sufficient as a control mechanism, as the S1 units can utilize the resources at their own discretion once they are allocated. The accountability channel serves as an essential complement to the resource channel, as it regulates the use of resources. Together, the accountability and resource channels form an integrated feedback loop, ensuring a balanced and viable system. Notably, an accountability channel without a corresponding resource channel is equally unsustainable, as it would hold individuals accountable without providing them with the necessary resources to fulfil their responsibilities. Therefore, the accountability and resource channels must always be considered in tandem to maintain the viability and effectiveness of the system.
- The corporate intervention channel: It encompasses activities that strike a balance between organisational cohesion and operational autonomy. It establishes the legal requirements, regulations, and rules that the operational units (S1) must follow. Moreover, by allocating or removing tasks and responsibilities from the S1 units, the metasystem defines the scope of variety that the S1 can handle. This highlights an important interdependency between the communication channels. When operational units are assigned more tasks and responsibilities, they may also require additional resources to fulfil them. Therefore, any viable corporate interventions must be reflected in the corresponding resource allocation channel.

4.3.3.5 Algedonic Channel - Variety Loop 5 (VL5): The algedonic raises alarms to trigger interventions outside normal regulatory channels. It includes activities that transfer signals from S1 to S5 directly, to manage risks requiring immediate attention from the metasystem, [\(Beer, S., 1979\)](#), [\(Beer, S., 1985\)](#), [\(Lowe, D., Espinosa, A. and Yearworth, M., 2020\)](#).

4.3.3.6 Recursive Governance - Variety Loop 6 (VL6): Recursive governance ensures that each embedded organisation operates as a viable system with appropriate autonomy for self-governance. Relationships between different levels of recursion ensure that each embedded system maintains its viability [\(Lowe, D., Espinosa, A. and Yearworth, M., 2020\)](#).

Previous research on the Viable System Model (VSM) has typically focused on identifying the five key subsystems within an organisation. However, to fully meet the requirements of the

VSM, it is essential to also establish the necessary information flows and key communication channels among these five subsystems. Schwaninger believed that for a social system to be viable, in addition to the five systems previously introduced, it requires the same interaction pattern as described in the models([Schwaninger, M., 1990](#)). Pérez Ríos emphasized that the diversity of communication channels and the transmission of information are fundamental characteristics of the Viable System Model (VSM).([Rios, P. J., 2012](#)). Consequently, comprehensive consideration must be given to all information flows and communication channels within the system in focus. The Viable System Model is a robust framework that is recognized for its ability to identify essential information flows among systems and the consequences of disrupting these flows. ([Williams, B. and Hummelbrunner, R., 2010](#)). Ensuring the viability of the system in focus necessitates a comprehensive consideration of the existence and quality of the 38 information flows within it as described in section 4.3.5 ([Achterbergh, J. and Vriens, D., 2002](#)); ([Preece, G., 2010](#)). With respect to communication channels, the existence, and quality of the channels in a system in focus must be considered, as described in section 4.3.4 ([Rios, P. J., 2012](#)).

4.3.4. Key VSM communication channels

The key VSM Systemic communication channels in Table 4.1 and Figure 4.2 (VSM Symbols are described in Appendix H) must be established to ensure the viability of an organisational system ([Rios, P. J., 2012](#)).

ID	Key VSM Systemic Communication Channels
C1	The relationship of each operating unit with its own management in S1
C2	Relationship of each operating unit in S1 with its own S2
C3	Relationship of each operational unit in S1 with its own environment
C4	The relationship between operational units themselves in S1
C5	Relationships among management of each operational unit in S1
C6	Relationship between each management of an elementary unit in S1 and S3
C7	Relationships among S2 of each S1 operational unit and corporate S2
C8	Relationship of each S1 operational unit with System 3*
C9	Algedonic channel - the relationship between S1 and S5 in case of crisis and high risks (outside the normal communication channels)

ID	Key VSM Systemic Communication Channels
C10	Relationship of S2 with S3
C11	Relationship of S3 with S3*
C12	Relationship of S3 with S4
C13	S3-S4 Homeostat
C14	Relationship of S4 and S5
C15	Relationship of S4 with future environment
C16	Relationship of S5 with S3-S4 Homeostat
C17	Relationship of the system in focus with the higher level of recursions and the lower level of recursions

Table 4. 1 Key VSM communication channels

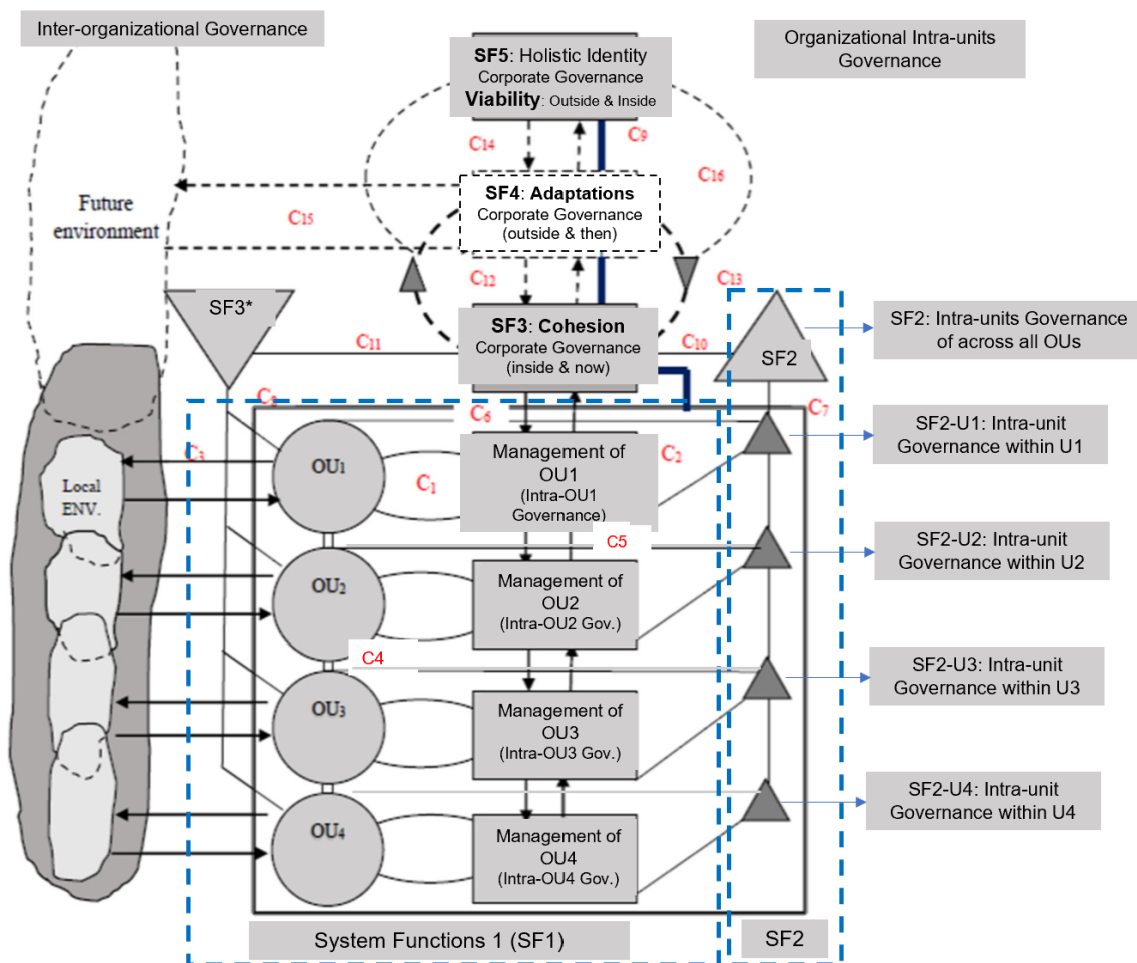


Figure 4. 2 Key VSM Systemic Communication Channels

4.3.5. Key VSM Information Domains (Flows)

This section illustrates and describes the key VSM information Domains or flows in Figure 4.3 (VSM Symbols are described in Appendix H) and Table 4.2. The key domains must be established to ensure the viability of an organisation. VSM can be viewed as an Information System with data and information flow within and across the five VSM systems (Achterbergh, J. and Vriens, D., 2002), (Beer, S., 1979), (Beer, S., 1981), (Beer, S., 1985), (Espejo, R. and Reyes, A., 2011), (Preece, G., 2010). Figure 4.3 shows data flows across VSM systems in Green.

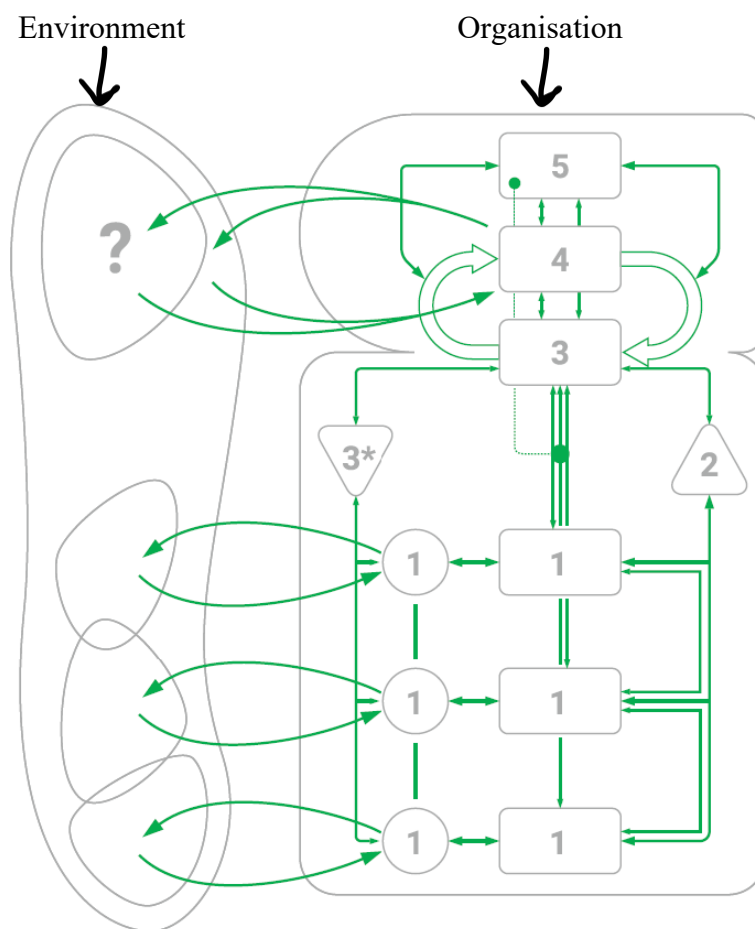


Figure 4. 3 VSM can be viewed as an Information System

ID	Information Flow and Description
ID1	External Environment Information generated by S1: This flow involves gathering data and insights about the external conditions and factors that affect the organisation, including market trends and requirements, regulatory changes, and competitor actions. It is crucial to understand the external environment and adapt accordingly. This flow identifies data and information necessary for executing tasks and activities in S1.

ID	Information Flow and Description
ID2	Goals Set by Performance in S1 - information generated by S1: These are objectives established by S1 based on the performance metrics of primary activities in S1. These goals help guide the efforts of various subsystems to align with overall organisational targets.
ID3	Organisational Goals generated by S5: The overarching goals and objectives of the organisation are derived from strategic planning processes set by S5. These goals provide a unified direction and purpose across all other systems (S1-S4).
ID4	Expected Performance Generated by S3 of the Primary Activity in S1: Targets and benchmarks set by S3 for the primary activities in S1. This information ensures that primary activities are aligned with organisational goals and performance standards.
ID5	Monitoring and Control Practices generated by S3: Procedures and mechanisms used by S3 to monitor and control the activities of S1. These practices are essential for ensuring efficiency, effectiveness, and compliance with organisational standards.
ID6	Goal and Performance Misalignment generated by S3: Information regarding discrepancies between the set goals and the actual performance of the organisation. The misalignments are identified by S3 to help S1 in taking corrective actions.
ID7	Causes and Consequences of Goal and Performance Misalignment Generated by S3 and S1: This flow involves analysing the reasons behind goal and performance misalignment and understanding their causes and consequences by S3 and S1.
ID8	Actions to Counter Goal and Performance Misalignment implemented by S1: Steps taken by S1 to address and correct performance issues, ensuring alignment with organisational goals.
ID9	Heuristics and Practical Approaches to Implement Counteractions - generated by S1: Guidelines or rules of thumb for implementing corrective actions in S1.
ID10	Operational Information - generated by S1: Day-to-day operational data and information necessary for executing tasks and activities in S1.
ID11	Anti-Oscillatory Measures generated by S2: Measures taken by S2 to prevent or reduce fluctuations and instability within S1.
ID12	Interdependencies Between S1 Activities - generated by S2: Information identified by S2 on how different activities within S1 are interconnected and affect each other.
ID13	Actual Oscillations generated by S2: Data on actual fluctuations and variances in S1 performance, identifying areas of instability by S2.
ID14	Actual Performance Loss Due to Oscillations generated by S2: Information identified by S2 on performance degradation caused by oscillations within S1.

ID	Information Flow and Description
ID15	Norms for Admitted Performance Loss Due to Oscillations (Goals for S2) - generated by S3: Accepted standards or thresholds set by S3 and used by System 2 for coordination for S1 performance loss due to oscillations.
ID16	Gap Between Norms for Admitted and Actual Performance Losses Due to Oscillations generated by S3: Discrepancies identified by S3 between accepted and actual S1 performance losses due to oscillations, highlighting areas for improvement for S2 activities.
ID17	Causes of the Gap Between Admitted and Actual Performance Losses Due to Oscillations - generated by S2: Reasons identified by S2 for differences between S1 expected and actual performance losses.
ID18	Experiences with Anti-Oscillatory Measures - generated by S2: Lessons learned generated by S2 from implementing measures to counter oscillations and improving future responses.
ID19	Problems and Needs of the Management of S1 Activities: Issues and requirements generated by the management of S1 and S3, addressing their operational needs and resources requirements.
ID20	Resource Allocation generated by S3: Information generated on how resources are distributed and utilized within the organisation.
ID21	Manipulation of External Environment by S4: External information identified by S4 that is required to strategically shape or respond to changes in the external environment, thereby enhancing the organisation's ability to adapt and remain responsive on a long-term basis.
ID22	Proposals for Innovation Made by S4: Suggestions for new ideas, products, or processes generated by S4 and shared with S5 and S3 to drive innovation and long-term adaptability to external requirements.
ID23	Desired Goals for S1 Based on Proposals for Innovation generated by S3: Strategic targets set by S3 for S1 derived from innovative ideas proposed by S4, aiming for organisational improvement to achieve long term goals.
ID24	Gap Between Desired and Current Goals of S1 generated by S3: S3 identification of gaps to be addressed and differences between the current state and desired future state of S1.
ID25	Required Capacity for Reorganisation of S1 Activities generated by S3: S3 identification of necessary resources and capabilities for restructuring activities in S1, to ensure readiness for future changes and improvements.

ID	Information Flow and Description
ID26	Actual Capacity for Reorganisation of S1 Activities generated by S3: S3 identification of current resources and capabilities available for restructuring activities in S1.
ID27	Gap Between Required and Actual Capacity for Reorganisation of S1 Activities generated by S3: S3 identification of discrepancies between needed and available resources for reorganisation in S1.
ID28	Auditing and Compliance information generated by S3*: S3* evaluation and verification of systems and processes, to ensure compliance to standards and guidelines to achieve organisational goals. Audit and compliance information is shared with S3 for corrective actions and improvements in S1.
ID29	Reviews by S3 of Proposals for Innovation: Evaluation of innovative proposals by S3, ensuring their feasibility and alignment with organisational goals. Information is shared with S4 and S5.
ID30	Finalized Plans for Adaptation of Organisational Goals generated by S3 and S4: S3 and S4 collaboration to approve strategies and plans for adjusting organisational objectives, ensuring alignment with external changes and balancing present and future strategic goals. Information is shared with S5.
ID31	Regulatory Measures to Counter Imbalance Between S3 and S4 generated by S5: Steps defined by S5 to address conflicts or imbalances between S3 and S4, to maintain stability.
ID32	Developments in the Relevant Environment of the Organisation: S4 identification of updates and changes in the external environment relevant to the organisation, ensuring responsiveness and sustainable adaptations.
ID33	Norms for Balance Between S3 and S4 generated by S5: S5 identification of standards for maintaining equilibrium between S3 and S4, ensuring coordinated actions to balance present and future goals.
ID34	Actual Imbalance Between S3 and S4 generated by S5: S5 identifies of current state of imbalance between S3 and S4 and determines areas needing attention.
ID35	Causes of Imbalance Between S3 and S4 generated by S5: S5 identification of Reasons for existing imbalances between S3 and S4 and understanding their causes.
ID36	Experiences with IF31 generated by S5: S5 identification of insights gained from implementing measures to balance S3 and S4, improving future responses.
ID37	Cultural Knowledge: Understanding of organisational culture and its impact on operations and performance (Espejo, R. and Reyes, A., 2011).

ID	Information Flow and Description
ID38	Algedonic Signals: Critical feedback signals related to pain (negative feedback) and pleasure (positive feedback), prompting adaptive responses (Beer, S., 1979).

Table 4. 2 Key VSM information domains (flows)

This comprehensive explanation of each information domain (flow) provides insight into their respective roles and significance in maintaining the viability of an organisation according to the Viable System Model (VSM). The table below (Table 4.3) summarizes the various information domains in the Viable System Model (VSM), showing where each type of information should be generated (G) and acted upon (A) within the different subsystems (S1 to S5) and the environment (Env).

(ID)	Information Domains	Env	S1	S2	S3	S3*	S4	S5
ID1	External environment information	G, A	A				A	
ID2	Goals set by performance and modus operandi of the primary activities in S1		G, A	A	A	A	A	
ID3	Organisational goals		A		A		A	G, A
ID4	Expected performance of the primary activity (goals for S1 activity)		A		G, A			
ID5	Monitoring and control practices by S3		A		G, A			
ID6	Goal and performance misalignment		A		G, A			
ID7	Causes and consequences of goal and performance misalignment		G, A		G, A			
ID8	Actions to counter goal and performance misalignment by S1		G, A					
ID9	Heuristics to implement counteractions		G, A					
ID10	Operational information		A	G, A				
ID11	Anti-oscillatory measures		A	G, A				
ID12	Interdependencies between S1 activities			G, A				
ID13	Actual oscillations			G, A				
ID14	Actual performance loss due to oscillations			G, A				

(ID)	Information Domains	Env	S1	S2	S3	S3*	S4	S5
ID15	Norms for admitted performance loss due to oscillations (goals for S2)			A	G, A			
ID16	Gap between norm for admitted and actual performance loss due to oscillations			A	G, A			
ID17	Causes of the gap between admitted and actual performance loss due to oscillations			G, A				
ID18	Experiences with anti-oscillatory measures			G, A				
ID19	Problems and needs of the management of S1 activities		G, A		G, A			
ID20	Resource allocation		A	G, A	G, A			
ID21	Manipulation of the external environment	A					G, A	
ID22	Proposals for innovation made by S4				A		G, A	A
ID23	Desired goals for S1 based on proposals for innovation				G, A			
ID24	Gap between desired and current goals of S1				G, A			
ID25	Required capacity for reorganisation of S1 activities				G, A			
ID26	Actual capacity for reorganisation of S1 activities				G, A			
ID27	Gap between required and actual capacity for reorganisation of S1 activities				G, A			
ID28	Auditing				A	G, A		
ID29	Reviews by S3 of proposals for innovation				G, A		A	A
ID30	Finalized plans for adaptation of organisational goals (a joint S3 and S4 product)				G, A		G, A	A
ID31	Regulatory measures to counter the imbalance between S3 and S4				A		A	G, A
ID32	Developments in the relevant environment of the organisation						G, A	
ID33	Norms for balance between S3 and S4							G, A
ID34	Actual imbalance between S3 and S4							G, A

(ID)	Information Domains	Env	S1	S2	S3	S3*	S4	S5
ID35	Causes of imbalance between S3 and S4							G, A
ID36	Experiences with regulatory measures to counter the imbalance between S3 and S4							G, A
ID37	Cultural knowledge	A	A	A	A	A	A	G, A
ID38	Algedonic signals	G, A	G, A	G, A	G, A	G, A	G, A	A

Table 4. 3 Key VSM Information Domains (Flows) within the VSM Systemic Context

VSM integrates an array of cybernetic and systemic stability concepts into a coherent framework, including feedback, communications, variety, recursion, viability, autonomy, self-regulation, self-organisation, and learning. The five VSM System Functions with their interconnecting communication links are depicted in Figure 4.4. The symbols in Figure 4.4. are described in Appendix H.

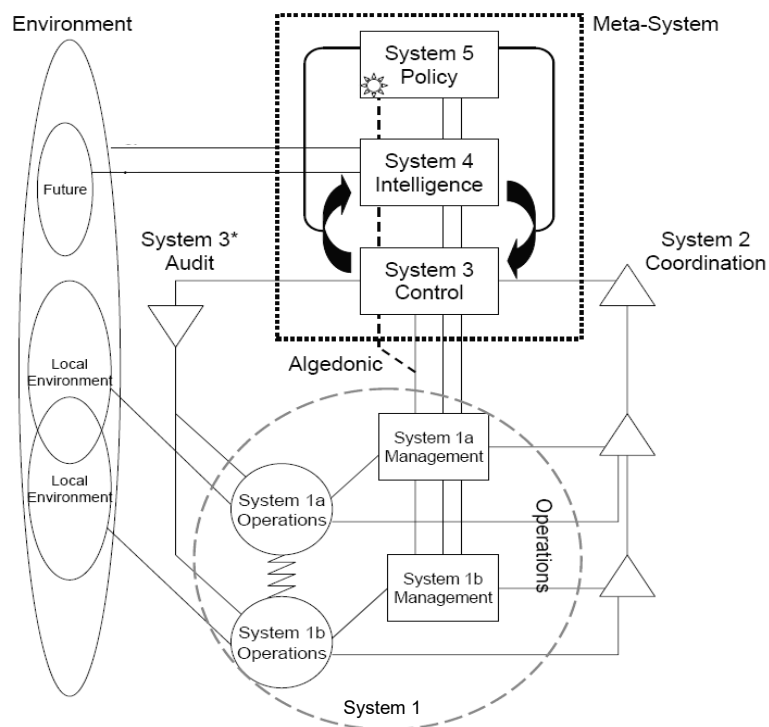


Figure 4. 4 The Viable System Model (Adapted from Beer, 1985)

VSM serves as a dynamic recursive framework (Figure 4.5 - symbols are described in Appendix H). The Viable System Model (VSM) is inherently recursive, meaning that every viable system is both contained within and contains other viable systems. Each embedded viable system interacts with its own unique local environment, which is a subset of the broader

environment of the overall system-in-focus. The fractal nature of the VSM allows for consistent modelling at different levels of granularity, where each viable system can be represented using the same fundamental structure. Within these recursive VSMs, organisational goals are also recursive, with higher-level viable system goals governing the settings and objectives of the nested, lower-level viable systems. VSM enables the design and evaluation of effective control mechanisms and communication channels, which provide the foundation for a comprehensive dynamic recursive system of governance in general and data governance in particular within a holistic context as explained below in section 4.4.

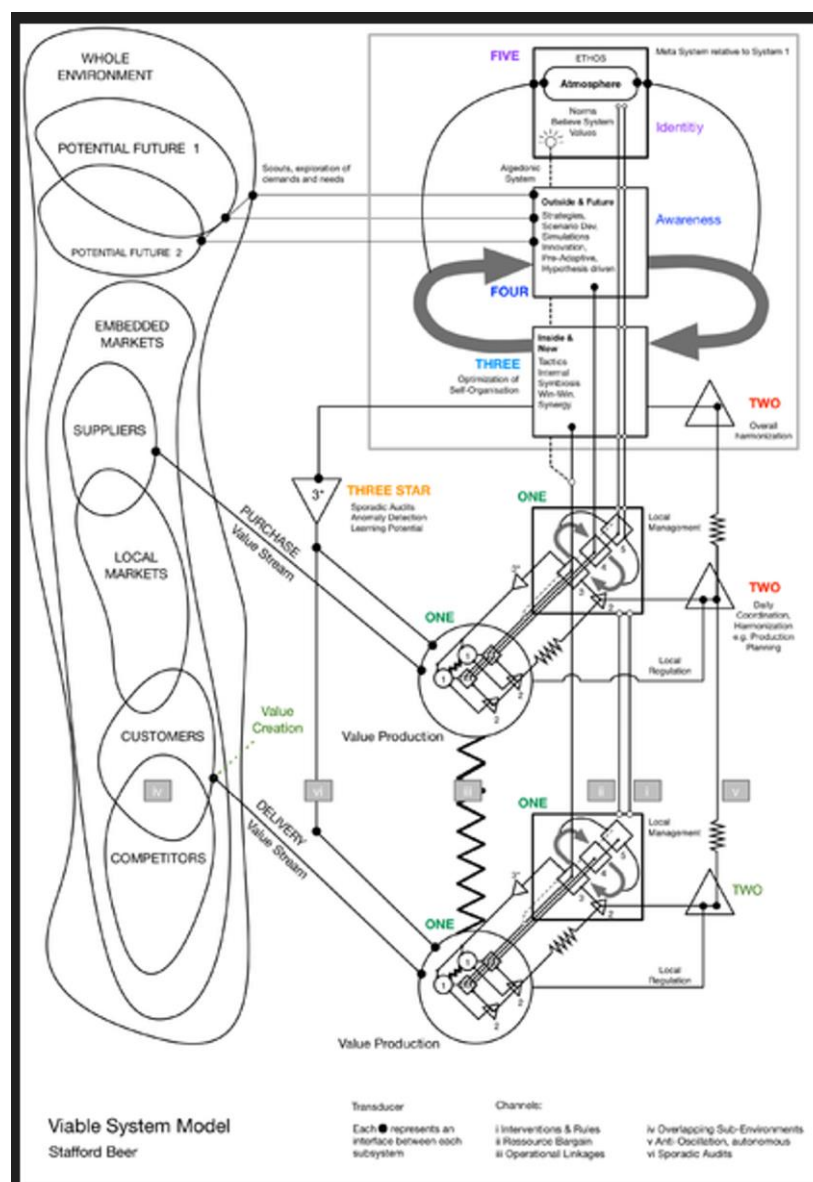


Figure 4. 5 VSM Dynamic Recursive Framework (e.g. two recursion levels)

4.4 Conceptualization of the Holistic Dark Data Governance Key Systemic Functions

This study proposes a holistic way of looking at data governance and in particular dark data governance by adapting the aspects of VSM organisational control and communication, namely governance. The VSM has been previously employed as a framework for analysing different models of corporate governance. VSM has been used to analyse and evaluate different models of corporate governance ([Davies, J., 2002](#)). VSM was also used to examine organisational information security([Gokhale, B. G. and Banks, D., 2004](#)). VSM was used as a reference for constructing a theoretical model of IT governance ([Peppard, J., 2005](#)). Other researchers used VSM to discuss theories of IT governance ([Dowse, A. and Lewis, E., 2009](#)), ([Huygh, T. and Haes, D. S., 2018](#)), and IT risk management ([Arghand, A. A., 2022](#)). However, none of the previous studies formulated a holistic model of Data governance based on the VSM. Beer (1979) defined a viable system as one that is capable of maintaining a separate existence, of surviving on its own. However, “survival” should not be interpreted in the limited sense of merely existing. In an increasingly competitive, complex world, survival can only be continuously realized through the processes of learning, adapting, and growing. Beer (1981) asserted that an organisation based on the VSM has the mechanisms and opportunities to grow and to learn, to evolve and to adapt – to become more and more potent in its environment. Similar language was used to encapsulate the central purpose of the “living company”, which exists primarily for its own survival and improvement to fulfil its potential and to become as great as it can be ([Geus, d. A., 1999](#)). Thus, surviving should not be construed in the narrow sense of merely existing since surviving involves learning, adapting, and growing. It has been argued that continuous growth and survival in the highly competitive global environment are the ultimate goals of value creation ([ITGL., 2005](#)). Thus, value creation contributes to organisational survival and growth.

However, value creation is only “one side of the coin” called survival. When striving to create value, the organisation must ensure that it does not assume risks that threaten its ongoing survival. Value creation and value preservation are consistent with Information Technology Governance Institute’s ([ITGL., 2003](#)) claim that governance is primarily concerned about two things: delivery of value to the business and mitigation of risks (i.e., dark data).

In short, value creation and value preservation (or risk management) are the ultimate source of organisation survival. A viable system survives and thrives; therefore, the attainment of value creation and value preservation (or risk management) are the primary purpose of a viable system of governance at large, and dark data governance in specific with its capability to handle

dark data risks. Taking a systemic view warrants a holistic view of the data governance construct, which is entirely in line with this research in the domain, which proposes data governance as a holistic set of systemic functions, and relational mechanisms. Taking a systemic view also requires thinking about the purpose of holistic data governance. The ultimate purpose of holistic data governance is generally seen as creating business value, while simultaneously mitigating dark data-related risks (Huygh, T. and Haes, D, S., 2018) to support the achievement of organisational goals ([Abraham, R., Schneider, J. and Brocke, v, J., 2019](#)),([Benfeldt, O., 2017](#)).

The digital data landscape has evolved to include more stakeholders and valuable assets beyond just data and information. This is because data lacks inherent will or intent, and people using technology ultimately shape and direct data. Therefore, data governance must be integrated with the governance of people and technology. Accordingly, governing data and the associated information technology work together to achieve organisational goals. Since governing data necessitates governing IT and IT-related risks, the concepts of systemic IT governance can be applied to holistic dark data governance ([Cheong, K, L. and Chang, V., 2007](#)), ([Arghand, A, 2022](#)).

Given the absence of prior studies that have formulated a holistic data governance framework, this study aims to propose a holistic data governance model. To achieve this objective, it is imperative to identify the key systemic dimensions integral to such a model. The process of identifying the systemic dimensions of holistic dark data governance is inherently complex and necessitates significant investigative efforts, involving various stakeholders. Based on the researcher's knowledge and the tertiary review presented in Chapter 3, there is a notable lack of published research that delineates the key systemic dimensions of a holistic model for dark data governance.

Sections 4.4.1, and 4.4.2, detail the application of the fundamental principles of the Viable System Model (VSM) to the conceptualisation of a holistic model for dark data governance (in integration with other relevant governance systems mainly IT and corporate governance), encompassing its systemic dimensions and functions.

4.4.1. VSM Underlying Concept and the Relevance to Holistic Dark Data Governance **Context: Viability**

The Viable System Model (VSM) is inherently recursive, meaning that every viable system is both contained within and contains other viable systems. Each embedded viable system interacts with its own unique local environment, which is a subset of the broader environment of the overall system-in-focus. The fractal nature of the VSM allows for consistent modelling

at different levels of granularity (recursion), where each viable system at any recursion level can be represented using the same fundamental structure. Within these recursive VSMs, organisational goals are also recursive, with higher-level viable system goals governing the settings and objectives of the nested, lower-level viable systems.

For data governance to be holistic, organisations need to embrace a dark data governance model embedded in a systemic context, and that requires thinking about positioning data governance within organisations where organisations are conceptualized as viable systems. The ultimate purpose of holistic data governance is generally seen as a strategic value to achieve business goals, while simultaneously mitigating data-related risks ([DAMA., 2017](#)), ([Abraham, R., Schneider, J. and Brocke, v, J., 2019](#)), ([Benfeldt, O., 2017](#)), ([Rees, V, I., 2007](#)). As such, the holistic data governance system supports the organisation's viability by proactively identifying potential strategic threats and opportunities within the digitally disruptive business environment ([Valentine, E. and Stewart, G., 2013](#)). It also counteracts the associated risks of dark data to enable the continuous creation and preservation of data-enabled business value ([Haes, D, S. and Grembergen, V, W., 2015](#)), thereby supporting the achievement of organisational goals. By consistently fulfilling this purpose, the holistic data governance model sustains the organisation's viability through the following two key mechanisms ([Arghand, A., 2022](#)), ([Huygh, T. and Haes, D, S., 2018](#)):

- Leveraging and controlling the organisation's digital data and related data governance systemic activities to support the business operational units and the achievement of organisational goals.
- Counteracting all risks related to dark data within the five VSM systemic functions and associated communication channels and information flows.

Section 4.4.2 presents the author's perspective on the key systemic dimensions and functions of a comprehensive model for holistic dark data governance, based on the compiled literature in Chapter 3 (Table 3.11) and Sections 4.2 and 4.3 in this Chapter.

4.4.2. Holistic Dark Data Governance Key Systemic Functions

This section outlines the key systemic functions of a holistic data governance model for managing dark data based on the critical success factors (Chapter 3 - Table 3.11, Chapter 4 - Section 4.2.1.) and the key constructs of the Viable System Model (Chapter 4 - Section 4.2.2, Section 4.3 and Section 4.4.1). The proposed model is summarised in Table 4.4. The below sections detail the key systemic functions of the proposed holistic dark data governance within the VSM context of organisations.

4.4.2.1 Holistic Dark Data Governance Systemic Function 1 (SF1) within VSM-S1: Operational Units (implementation)

SF1 includes defining, deploying and sustaining all the data governance systemic function that supports the operational units in S1 to achieve their organizational goals. According to the VSM theories, the embedded operational units within S1 must be independent viable systems, capable of existing on their own. Operational units are defined as the systemic functions responsible for fulfilling the organisation's purpose, while data management is considered a supportive systemic activity. The purpose of a manufacturer is to manufacture products, not manage data and information systems. The data management and Information Technology (IT) and their governance units facilitate business operations. Given that the data governance unit is not an operational unit, it cannot be a viable system in its own right ([Beer, S., 1985](#)). As a general rule, common data governance systemic functions that contribute to the synergy of operational units are always representative of SF3 functions([Beer, S., 1979](#)) - Section 4.4.2.3. Rather than viewing the data governance, data management, and IT functions as self-contained units with their own goals, they should be seen as supporting roles that exist to help the organisation achieve its business objectives. When the data management, data governance, IT, and IT governance functions are all treated as support systems, it becomes easier to align them with the overall business needs. This helps resolve the long-standing challenge of integrating these functions with the core business ([Beer, S., 1979](#)). In this context, data governance serves as a supporting systemic function (SF1) for the business operations within VSM S1, aimed at ensuring the viability of S1 and its embedded viable systems. This is because data governance leverages the organisation's digital data assets and related activities, while also addressing and mitigating the risks associated with dark data encountered while implementing the business operational activities within S1. To meet its purpose of creating and preserving data business value, data governance leverages the digital data assets and relevant systemic data governance activities in a controlled way especially the management of dark data risks within S1 ([ISO/IEC., 2008](#)), ([Huygh, T. and Haes, D, S., 2018](#)). Identifying dark data types, maintaining the current dark data risk profile, and reporting it at specific intervals is a key systemic action of SF1 ([Arghand, A, A., 2022](#)).

Below are the key communication channels (Rios, P, J., 2012) and information flows (Achterbergh, J. and Vriens, D., 2002); (Preece, G., 2010) within SF1 that are relevant to holistic data governance (HDG) and dark data systemic activities.

- **HDG Communication Channels within SF1:**
 - **HDG C1:** The communication of each operating unit with its own management in S1 related to data governance and dark data handling systemic activities
 - **HDG C4:** The communication between operational units themselves in S1 related to data governance and dark data handling systemic activities
 - **HDG C5:** The communication among management of each operational unit in S1 related to data governance and dark data handling systemic activities
- **HDG Key Systemic Information Flows within SF1:**
 - **HDG IF8: Actions to Counter Goal and Performance Misalignment implemented by SF1:** Steps taken by SF1 to address and correct performance issues related to data governance and dark data handling systemic activities, ensuring alignment with organisational goals
 - **HDG IF9: Heuristics and Practical Approaches to Implement Counteractions - by SF1:** Guidelines or rules of thumb for implementing corrective actions related to data governance and dark data handling systemic activities in SF1.
 - **HDG IF10: Operational Information - generated by SF1:** Identification of day-to-day operational data and information necessary for executing tasks and activities in S1 and counteracting dark data.

Given the above, the data governance systemic function (SF1) supports S1 operational units by managing digital data assets and mitigating dark data risks. SF1 is not a viable system on its own but supports organisational goals by aligning data governance with business operations. Key actions include identifying dark data, maintaining dark data risk profiles, and regular reporting to other relevant systemic functions as necessary. Communication channels and information flows within S1 are essential for effective data governance and dark data management to support the achievement of operational and organisational goals.

4.4.2.2 Holistic Dark Data Governance Systemic Function 2 (SF2) within VSM-S2: Co-ordination and Harmonization

SF2 includes defining, deploying and sustaining all data governance and IT governance systemic functions within S2 that support the coordination of the operational business activities of S1 and the achievement of operational and organisational goals. They represent an auto-regulation process to handle oscillations arising from interactions within or between embedded viable systems ([Beer, S., 1979](#)) regarding data requirements and dark data risks with the

relevant technologies utilized. SF2 mechanisms can reflect data governance managerial decisions but do not make them ([Beer, S., 1985](#)). The purpose of SF2, Coordination, is to promote organisational synergies through cooperation ([Brocklesby, J., Cummings, S. and Davies, J., 1995](#)). SF2 focuses on the various coordination mechanisms related to dark data governance (e.g., guidelines, policies, rules, standards, training, meeting schedules and relevant technologies) that ensure the operational units work together harmoniously rather than in conflict ([Huygh, T. and Haes, D. S., 2019](#)). The key principle for designing these coordination mechanisms is that the operational units in S1 should view them as supportive functions, not as orders to comply with. The operational units in S1 should adhere to the policies, standards, and technologies because they provide tangible benefits to businesses in handling data and counteracting dark data, not because they are required to do so ([Lewis, E. and Canberra, U., 2010](#)).

Given the above, SF2 focuses on data governance systemic functions in integration with IT governance systemic functions within S2 that support the coordination of S1 operational activities. It handles oscillations from interactions between viable systems regarding digital data requirements and dark data risks, promoting synergies through cooperation. SF2 mechanisms, such as guidelines, procedures, and policies, ensure operational units work harmoniously. These mechanisms are viewed by S1 as supportive rather than obligatory since they are crucial to the achievement of operational and organisational goals.

4.4.2.3 Holistic Dark Data Governance Systemic Function 3 (SF3) within VSM-S3: Control (Cohesion and Autonomy)

SF3 includes defining, deploying and sustaining data governance systemic functions and activities to control the operations of SF1 within S1 recursive viable systems and support the achievement of organisational goals and S1 embedded sub-goals ([Heylighen, F. and Joslyn, C., 2003](#)), ([Beer, S., 1985](#)). They balance the autonomy of all embedded viable systems with overall cohesion ([Lowe, D., Espinosa, A. and Yearworth, M., 2020](#)), focusing on the present data governance systemic functions and taking in consideration the integration with relevant data and information technologies (IT) ([Reynolds, M. and Holwell, S., 2010](#)). The key systemic data governance roles located within SF3 are typically the level of the Chief Executive Officer (CEO), the business executives, and the Chief Information Officer (CIO) or equivalent roles based on the level of recursion of this study (organisation - explained in section 4.4.2.7). The corporate CIO or the equivalent role occupies a critical, but not an absolute, position. The

organisational actors identified are consistent with the key governance roles identified by the IT Governance Institute; namely: the CEO, business executives, and the CIO roles ([ITGI, 2003](#)). SF3 involves several key practices (Table 3.11 – CSF2) to ensure data is managed efficiently and supports business objectives. Data stewardship assigns responsibilities for managing data throughout its lifecycle, maintaining its integrity within a defined business scope. Data lifecycle management ensures data handling aligns with business and regulatory requirements, remaining relevant and compliant from creation to retirement. Establishing data classification standards helps organise data based on sensitivity and business value, ensuring appropriate protection and management. Maintaining a comprehensive data inventory supports the organisation, management, and protection of data, facilitating effective governance. Addressing dark data begins with identifying its sources within the organisation and classifying it based on sensitivity, value, and relevance to prioritise management efforts and protect critical assets. These practices collectively enhance data governance and optimise organisational data management. SF3 defines and sustains corporate roles, incident management, corporate policy development, data quality control, data access controls, metadata management, and resource allocation to ensure cohesion across the organisation (Table 3.11 – CSF5). SF3 establishes continuous improvement processes (from information collected by SF3* - Section 4.4.2.4), defines and tracks KPIs, regularly assesses governance maturity, and ensures ongoing evaluation to keep governance practices relevant and effective (Table 3.11 – CSF11).

Below are the key HDG information flows (Achterbergh, J. and Vriens, D., 2002); (Preece, G., 2010) within SF3 that are relevant to data governance and dark data systemic activities.

- **HDG Key Systemic Information Flows within SF3:**
 - **HDG IF23: Desired Goals for S1 Based on Proposals for Innovation generated by SF3:** Strategic targets related to data governance and dark data handling systemic activities set by SF3 for SF1 derived from innovative ideas proposed by SF4, aiming for organisational improvement to achieve long-term goals.
 - **HDG IF24: Gap Between Desired and Current Goals of SF1 generated by SF3:** SF3 identification of gaps related to data governance and dark data handling systemic activities to be addressed and differences between the current state and desired future state of SF1.
 - **HDG IF25: Required Capacity for Reorganisation of SF1 Activities generated by SF3:** SF3 identification of necessary resources and capabilities related to data governance and dark data handling systemic activities for restructuring activities in SF1, to ensure readiness for future changes and improvements.

- **HDG IF26: Actual Capacity for Reorganisation of SF1 Activities generated by SF3:** SF3 identification of current resources and capabilities, related to data governance and dark data handling systemic activities, available for restructuring activities in SF1.
- **HDG IF27: Gap Between Required and Actual Capacity for Reorganisation of SF1 Activities generated by SF3:** SF3 identification of discrepancies, related to data governance and dark data handling systemic activities, between needed and available resources for reorganisation in SF1.

SF3 focuses on the following data governance systemic functions in integration with relevant technologies ([Beer, S., 1981](#)),([Beer, S., 1979](#)):

- Management of corporate data requirements and corporate dark data risk management systemic activities and solutions, particularly those related to data governance policies, procedures and guidelines regarding data governance domains([Weill, P. and Ross, W. J., 2004](#)): Data Architecture, Data Quality, Metadata, Data Security, Reference & Master Data, Data Warehousing/Business Intelligence/Artificial Intelligence, Data Modelling & Design, Document & Content Management, Data Storage & Infrastructure/Operation, Data Integration & Interoperability (description in an Appendix I)
- Corporate intervention (compliance management): Define, and sustain requirements
- Compliance with legal, regulatory, and ethical obligations (e.g., privacy legislation) regarding data governance is governed via SF3. The principles and policies issued by the Board and CEO (and other business leaders) are used to guide the development of the policies formulated by the functional leaders such as the CIO. Therefore, when the CIO is crafting the principles and policies to govern dark data function, they must accord with those formulated for the corporation as a whole. SF3 focuses on activities that strike a balance between organisational cohesion and operational autonomy. It establishes the legal requirements, regulations, and rules that the operational units (S1) must follow. Moreover, by allocating or removing tasks and responsibilities from the SF1 units, the metasystem defines the scope of variety that the SF1 can handle. This highlights an important interdependency between the communication channels. When operational units are assigned more tasks and responsibilities, they may also require additional resources to fulfil them. Therefore, any viable corporate interventions must be reflected in the corresponding resource allocation channel.
- Resource bargaining (resource management, accountability, and performance management): The resource bargaining aspect encompasses the allocation of various resources, such as financial, human, knowledge-based, training, and time-related, to the

operational units (SF1) related to data governance systemic activities. The more resources these units receive, the more capable and flexible they become in their actions in handling data requirements and counteracting dark data risks. Conversely, a restriction of resources diminishes the scope and adaptability of the SF1 units to support the achievement of business objectives. However, the resource allocation alone is not sufficient as a control mechanism, as the SF1 units can utilize the resources at their own discretion once they are allocated. The accountability channel serves as an essential complement to the resource channel, as it regulates the use of resources. Together, the accountability and resource channels form an integrated feedback loop, ensuring a balanced and viable system. Notably, an accountability channel without a corresponding resource channel is equally unsustainable, as it would hold individuals accountable without providing them with the necessary resources to fulfil their responsibilities. Therefore, accountability and resource channels must always be considered in tandem to execute the dark data governance activities successfully and maintain the viability and effectiveness of the system.

- The primary purpose of resource bargaining is to provide SF3 with the means to regulate, or govern, the activities of the operational units in order to realize enterprise-wide synergies. Essentially, SF3 seeks to govern the data governance projects and dark data risk management activities on a “resource-result” basis. SF3 and the business units in S1 agree on the desired outcomes and the resources to achieve agreed objectives. The performance against those objectives is reported by SF1 to SF3 and S3 (i.e., performance management). Performance reports provide the mechanism through which SF3 can hold the business units in S1 accountable for achieving their assigned objectives. As Stafford Beer noted, the governing mode of management is centred on accountability ([Beer, S., 1985](#))

Given the above, SF3 within S3 encompasses data governance systemic functions and activities to define, deploy and sustain SF1 operations within S1 recursive viable systems, supporting organisational goals, S1 sub-goals and overall organisational viability. It support balancing the autonomy of embedded viable systems with overall cohesion. SF3 systemic functions integrate with corporate and IT Governance systemic functions and include compliance management, legal and regulatory adherence, resource allocation, and performance management to ensure effective data governance.

4.4.2.4 Holistic Dark Data Governance Systemic Function 3* (SF3*) within VSM-S3*: Audit and Compliance

SF3* within S3 encompasses defining, deploying and sustaining the systemic functions related to dark data governance auditing. This enables SF3 within S3 to directly acquire the necessary information about dark data challenges and data governance support operations (SF1) from the S1 operational units ([Beer, S., 1985](#)). SF3 regularly monitors and audits data governance processes, conducts data protection impact assessments, ensures auditable processes, including third-party governance audits, and tracks dark data governance metrics and KPIs for improvement (Table 3.11 – CSF6). SF* also ensures business operations (within S1) compliance with governance policies, standards, and regulations (Table 3.11 – CSF3).

Below are the key communication channels (Rios, P, J., 2012) and information flows (Achterbergh, J. and Vriens, D., 2002); (Preece, G., 2010) with S3* that are relevant to holistic data governance and dark data systemic activities.

- **HDG Key Systemic Communication Channels within SF3*:**
 - **HDG C11:** The communication of SF3 with SF3* related to data governance and dark data handling systemic activities of auditing and compliance requirements
 - **HDG C8:** The communication of each SF1 operational unit with SF 3* related to data governance and dark data handling systemic activities
- **HDG Key Systemic Information Flows within SF3*:**
 - **HDG IF28:** Auditing and Compliance information generated by SF3*: conducting independent evaluation and verification of systems and processes related to data governance and dark data handling systemic activities for SF1 within S1, ensuring accuracy and reliability. SF3* evaluation and verification of systems and processes, to ensure compliance with standards and guidelines to achieve organisational goals. Audit and compliance information is shared with SF3 and S3 for corrective actions and improvements in SF1.

Given the above, SF3* within S3* includes data governance auditing functions that enable SF3 within VSM S3 to gather information about dark data challenges and governance operations from S1 operational units. Key HDG communication channels involve auditing and compliance coordination between SF3, SF3*, SF1, and VSM operational S1 units. They focus on auditing and compliance evaluations to ensure accuracy and adherence to data governance standards, with results shared for corrective actions. This supports the achievement of operational goals.

4.4.2.5 Holistic Dark Data Governance Systemic Function 4 (SF4) within VSM-S4: Intelligence/Planning

SF4 includes defining, deploying and sustaining data governance systemic functions and activities within S4 to sense opportunities and threats (dark data) related to data needed by organisations in the system's environment that could threaten its viability ([Espejo, R. and Harnden, R., 1989](#)). SF4 manages potential future states of the system, does future-oriented tasks, and engages in external communication (e.g. Research and Development, Market research, corporate planning)). SF4 maintains a self-referential model of the organisational system that continuously refers to and modifies itself to ensure it remains effective and aligned with its objectives, enhancing its resilience and adaptability ([Beer, S., 1985](#)), ([Reynolds, M. and Holwell, S., 2010](#)). In the context of organisational theory and cybernetics, a self-referential model, like the Viable System Model (VSM), uses feedback loops to ensure the system's components are aligned with its goals and can adapt to changes both internally and externally. SF4 ensures that dark data governance is aligned with the organisation's business strategy, leveraging data for business intelligence, innovation, and supporting long-term business goals (Table 3.11 – CSF1). SF4 develops, deploy and sustain data governance strategy and long-term orientation in integration with corporate and IT Governance to support the achievement of the organisation's long-term goals.

4.4.2.6 Holistic Dark Data Governance Systemic Function 5 (SF5) within VSM-S5: Policy (Identity and Closure)

SF5 is the ultimate decision-making within a recursion of the viable system thereby providing logical closure to it within the system-in-focus S5 ([Beer, S., 1985](#)). SF5 includes defining, deploying and sustaining all the systemic functions that support creating and sustaining the system's identity, cohesion, long-term viability, and achieving organisational goals ([Beer, S., 1979](#)). SF5 includes defining, deploying and sustaining all the systemic functions within S5 that set the system's overall data governance direction, policies, values, and purpose, and monitor the feedback loop between current (SF3) and future (SF4) governance systemic functions to ensure balance between them ([Beer, S., 1985](#)), ([Espejo, R. and Gill, A., 2011](#)), ([Reynolds, M. and Holwell, S., 2010](#)). As such, SF5 balances between internal and external perspectives to support the achievements of present operational and long-term organisational goals.

4.4.2.7 Holistic Dark Data Governance Systemic Function integration at different levels of recursions (SF6): Recursivity

Recursive governance ensures that each embedded organisation operates as a viable system with appropriate autonomy for self-governance. Relationships between different levels of recursion ensure that each embedded system maintains its viability ([Lowe, D., Espinosa, A. and Yearworth, M., 2020](#)). All HDG Channels of Communication of the system in focus are repeated at lower levels of recursions where SF1 (within VSM S1) becomes SF5 (within VSM S5) at the lower level. All communications are repeated at higher levels of recursions where SF5 (within VSM S5) becomes SF1 (within VSM S1) at the higher level. As such, all data governance systemic functions at different levels of recursions are integrated. Controlling data assets and their related digital activities should be established at different levels of granularity ([Haes, D, S. and Grembergen, V, W., 2015](#)), ([Gaertner, J., Green, P. and Heales, J., 2012](#)). For instance, at the inter-organisational level, at the corporate level, at the business domain level, at the project level, at the project task level, etc. Starting from (corporate-level) dark data governance (including dark data risks governance & management) gradually flows into digital data management ([Peterson, R., 2004](#)) and enables the model to be applied to any scale of analysis within the organisational embedded viable systems ([Lewis, E. and Canberra, U., 2010](#)).

Identifying the system-in-focus (i.e., the level of recursion) is the first critical step in using the VSM to design or diagnose an organisation ([Jackson, C, M., 2003](#))([Lewis, E. and Canberra, U., 2010](#)). Although the functions of the component systems of a viable system remain invariant, the specific means of their realization do not at different levels of recursion. For example, System 5 is the policy function of the VSM, i.e., it is responsible for establishing the policies, or principles of action, that the viable system must adhere to. Within the context of dark data governance, the specific mechanisms through which SF5 activities are enacted may vary depending on the level of analysis. For instance, if the focus is at the corporate level, SF5 would primarily be manifested through the board of directors as the structural mechanism. Conversely, if the analysis is centred on a data governance project, SF5 would be enacted via the establishment of a project steering committee. Although the fundamental function of SF5 remains consistent, the particular structural means by which it is realized can change based on the level of the recursion under consideration. To develop a model of data governance that provides a holistic corporate context, this research adopts the corporation as the specific unit of analysis. As such, interactions with other different levels of recursions are outside the scope of this study.

Given the above, recursive governance ensures that each embedded organisation operates as a viable system with appropriate autonomy for self-governance, maintaining viability through integration at different levels of recursion. Key HDG Communication channels are repeated across levels, integrating data governance functions. Data governance should be controlled at various levels of granularity, from corporate to project tasks. All governance (data, IT and corporate) systemic functions at different levels of recursions are integrated to support the viability and the achievement of operational and organisational embedded goals (Table 3.11 – CSF8). SF6 involves defining, implementing, and maintaining all the systemic functions necessary to ensure the integration and alignment of all governance domains within a set scope and well-defined purpose. To develop a model of data governance that provides a holistic corporate context, this research adopts the organization scope as the specific unit of analysis.

4.4.2.8 Holistic Dark Data Governance (Operational & Strategic) Requisite Variety - Systemic Functions (SF7)

SF7 includes defining, deploying and sustaining all the systemic functions that support the organisation to manage the complexity of its environment through SF1 and SF4. The VSM system-in-focus communicates with its environment through SF1 with its embedded viable systems and through SF4 with the total environment. This communication involves both short-term and long-term data governance activities focused on identifying and responding to data governance present and anticipated requirements and dark data threats within the system's environment to achieve organisational goals ([\(Beer, S., 1979\)](#), [\(Beer, S., 1985\)](#)). This also involves creating sufficient internal variety to match the variety and complexity of the external environment, allowing the organisation to effectively respond to changes and uncertainties related to dark data risks and data governance requirements. The current complex business environment is characterized by digital disruptions and digital transformations ([\(Valentine, E. and Stewart, G., 2013\)](#)), which are major variety/complexity sources for organisations. Potential dark data threats and risks and opportunities in such a turbulent business environment need to be detected and readily responded to ([\(Overby, E., Bharadwaj, A. and Sambamurthy, V., 2006\)](#)). The dark data governance system must possess sufficient internal variety to effectively manage data assets and mitigate dark data risks in response to external digital disruptions and emerging data regulations. This internal variety is essential to establish the requisite variety necessary to support the organisation's viability.

Below are the key communication channels (Rios, P, J., 2012) and information flows (Achterbergh, J. and Vriens, D., 2002); (Preece, G., 2010) within SF7 that are relevant to holistic data governance and dark data handling systemic activities.

- **HDG Key Communication Channels within SF7:**
 - **HDG C3:** The communications of each operational unit in SF1 with its own environment related to data governance and dark data handling systemic activities
 - **HDG C15:** The relationship of SF4 with future environment related to data governance and dark data handling systemic activities
- **HDG Key Information Flows within SF7:**
 - **HDG IF1: External Environment Information needed by SF1:** This flow involves gathering data and insights by SF1 about the external conditions and factors that affect the organisation, including market trends and requirements, regulatory changes, and competitor actions relevant to data governance and dark data systemic activities. It is crucial for understanding the external environment and adapting on a timely and short-term basis. This flow identifies data and information necessary for executing systemic activities in SF1
 - **HDG IF21: Manipulation of External Environment by SF4:** External information identified by S4 relevant to data governance and dark data systemic activities. Data is required to strategically shape or respond to changes in the external environment, thereby enhancing the organisation's ability to adapt and remain responsive on a long-term basis.
 - **HDG IF32: Developments in the Relevant Environment of the Organisation:** SF4 identification of updates and changes in the external environment relevant to the organisation, ensuring responsiveness and sustainable adaptations relevant to data governance and dark data systemic activities

The identification of updates and changes in the external environment (S4) is crucial for ensuring responsiveness and sustainable adaptations relevant to data governance and dark data systemic activities. This process involves continuously monitoring external factors that may impact the organisation, thereby enabling it to adapt its strategies and practices accordingly. The ability to promptly respond to such changes is essential for maintaining effective data governance and managing dark data within the organisational framework. This approach ensures that the organisation remains agile and can sustainably manage its data assets in a constantly evolving external environment ([Ladley, J., 2012](#)), ([Pinto, K, J. and Prescott, E, J., 1988](#)).

Given the above, to manage environmental complexity, an organisation must create sufficient internal variety to match external variety, allowing it to respond effectively to changes and uncertainties. The current business environment, marked by digital disruptions and transformations, demands this adaptability. Detecting and responding to dark data threats and opportunities is crucial. The dark data governance system must have an adequate internal variety to manage data assets and mitigate risks, ensuring organisational viability. SF1 and SF4 communication channels and information flows with the environment facilitate short-term and long-term data governance activities, enabling the organisation to remain agile and responsive to environmental changes. This supports the achievement of operational and strategic organizational goals.

4.4.2.9 Holistic Dark Data Governance Inter-Operational Management (Cohesion): Balance of Autonomy and Control Systemic Functions (SF8)

Ensuring that operational units (S1) have enough autonomy to be effective and responsive while maintaining sufficient control through S1 support activities (SF1), coordination (SF2), and control (SF3) functions to ensure alignment of all data governance and dark data handling activities with the organisation's overall strategy and objectives. This includes communications among S1, S2, and S3 to manage operational complexity and enable effective decision-making through harmonization, self-regulation, and synergies in all systemic functions related to data governance and dark data handling ([Lowe, D., Espinosa, A. and Yearworth, M., 2020](#)).

Below are the key communication channels (Rios, P, J., 2012) and information flows (Achterbergh, J. and Vriens, D., 2002); (Preece, G., 2010) within SF8 that are relevant to holistic data governance and dark data systemic activities.

- **HDG Key Communication Channels among SF1, SF2, and SF3 within SF8:**
 - **HDG C2:** The relationship of each operating unit in SF1 with its own SF2 related to data governance and dark data handling systemic activities
 - **HDG C6:** The relationship between each management of an elementary unit in SF1 and SF3 related to data governance and dark data handling systemic activities
 - **HDG C7:** The relationships between SF2 of each SF1 operational unit and corporate SF2 related to data governance and dark data handling systemic activities
 - **HDG C10:** The relationship of SF2 with SF3 related to data governance and dark data handling systemic activities

- **HDG Key Information Flows within SF8:**
 - **HDG IF2: Goals Set by Performance in SF1 - information generated by SF1:** These are objectives generated by SF1 based on the performance metrics of primary and support systemic activities in SF1. These goals help guide the efforts of various subsystems (SF1, SF2, SF3 & SF4) to align primary and data governance and dark data handling (support) systemic functions with overall organisational targets.
 - **HDG IF4: Expected Performance generated by SF3 of the Governance Support Activity in SF1:** Targets and benchmarks set by SF3 for support activities for S1 primary activities related to data governance and dark data handling systemic functions in SF1. This information ensures that SF1 support and S1 primary systemic activities are aligned with organisational goals and performance standards.
 - **HDG IF5: Monitoring and Control Practices generated by SF3:** Procedures and mechanisms used by SF3 to monitor and control the support (SF1) systemic activities within S1 primary activities. These practices that are related to data governance and dark data handling systemic functions are essential for ensuring efficiency, effectiveness, and compliance with organisational governance standards.
 - **HDG IF6: Goal and Performance Misalignment generated by SF3:** Information regarding discrepancies between the set goals and the actual performance of governance support systemic activities within S1 of the organisation. The misalignments are identified by SF3 to help SF1 in taking corrective actions.
 - **HDG IF7: Causes and Consequences of Goal and Performance Misalignment generated by SF3 and SF1:** This flow involves investigating the reasons behind goal and performance misalignment of governance support systemic activities (supports S1 primary activities) and understanding their causes and consequences by SF3 and SF1.
 - **HDG IF11: Anti-Oscillatory Measures generated by SF2 and agreed with SF1:** Measures taken by SF2 to prevent or reduce fluctuations and instability within SF1 related to data governance and dark data handling systemic functions.
 - **HDG IF12: Interdependencies Between SF1 Activities - generated by SF2:** Information identified by SF2 on how different activities related to data governance and dark data handling within SF1 are interconnected and affect each other in supporting S1 primary activities.
 - **HDG IF13: Actual Oscillations generated by SF2:** Data on actual fluctuations and variances in SF1 (within S1) support systemic functions related to data governance and dark data management performance. SF2 also identifies areas of instability.

- **HDG IF14: Actual Performance Loss Due to Oscillations generated by SF2:** Information identified by SF2 on operational systemic functions and data governance support systemic functions performance degradation caused by oscillations within S1 primary activities.
- **HDG IF15: Norms for Admitted Performance Loss Due to Oscillations (Goals for SF2) - generated by SF3:** Accepted standards or thresholds set by SF3 and used by SF2 for coordination for SF1 operational systemic functions and data governance support systemic functions performance loss due to oscillations within S1 primary activities.
- **HDG IF16: Gap Between Norms for Admitted and Actual Performance Losses Due to Oscillations generated by SF3:** Discrepancies identified by SF3 between accepted and actual SF1 (Governance secondary systemic functions within S1) performance losses due to oscillations, highlighting areas for improvement for SF2 activities.
- **HDG IF17: Causes of the Gap Between Admitted and Actual Performance Losses Due to Oscillations - generated by SF2:** Reasons identified by SF2 for differences between SF1 (secondary systemic functions) expected and actual performance losses within S1 primary activities.
- **HDG IF18: Experiences with Anti-Oscillatory Measures - generated by SF2:** Lessons learned generated by SF2 from implementing measures to counter oscillations related to data governance and dark data handling systemic functions and improving future responses.
- **HDG IF19: Problems and Needs of the Management of SF1 Activities:** Issues and requirements generated by the management of SF1 and SF3, addressing their operational needs and resource requirements related to data governance and dark data handling systemic functions.
- **HDG IF20: Resource Allocation generated by SF3:** Information generated on how resources are distributed and utilized within the organisation related to data governance and dark data handling systemic functions.

Given the above, defining, deploying and sustaining SF8 systemic functions to integrate SF1, SF2, and SF3 is crucial to support operational units (S1) in achieving their organizational goals. Integration requires balancing autonomy with control through SF1 data governance support activities to S1 operational units, adequate SF2 data governance coordination, and adequate

SF3 data governance control. This alignment is critical for harmonizing all data governance and dark data handling activities with the organisation's strategy and objectives. Key HDG systemic communication channels (C2, C6, C7, C10) and HDG information flows (IF2, IF4, IF5, IF6, IF7, IF11, IF12, IF13, IF14, IF15, IF16, IF17, IF18, IF19, IF20) support the integration and alignment of data governance and dark data activities within the organisation to support the operational complexity and enhances decision-making through self-regulation and synergy. This supports the achievement of organisational operational goals.

4.4.2.10 Holistic Dark Data Governance Adaptability, Learning and Change Management Systemic Function (SF9)

SF9 includes defining, deploying and sustaining all systemic functions that integrates SF3, SF4, and SF5 (Metasystem). The ability of the organisation to adapt to changes in its environment and to learn from its experiences is crucial for its long-term viability and achievement of operational and organisational goals. This involves double-loop learning, where the organisation not only adjusts based on feedback but also questions and revises its underlying policies and goals. The variety loop between SF3 and SF4 balances the relationship between the present and the future, involving strategic decision-making ([Reynolds, M. and Holwell, S., 2010](#)). SF5 monitors this loop to ensure cohesion, and alignment with the system's overall direction, values, and purpose ([Beer, S., 1985](#)), ([Espejo, R. and Gill, A., 2011](#)). It combines internal and external perspectives on feasible and desirable future developments, to support data governance strategy development for the organisation ([Lowe, D., Espinosa, A. and Yearworth, M., 2020](#)). The metasystem comprising SF3, SF4, and SF5, provides the organisation with data governance decision-making capabilities. It balances present and future orientations and internal and external perspectives to maintain homeostasis. The command axis (S5, S4, and S3) includes ([Beer, S., 1979](#)), ([Beer, S., 1972](#)), ([Reynolds, M. and Holwell, S., 2010](#)), ([Lowe, D., Espinosa, A. and Yearworth, M., 2020](#)): the resource bargaining and accountability channel and the corporate intervention channel related to data governance and dark data handling across SF3, SF4, and SF5. SF9 activities include adapting to environmental changes, adopting best practices, implementing agile governance, developing long-term data governance strategies, managing dark data risks proactively, and aligns with organisational strategic goals (Table 3.11 – CSF7). SF9 manages changes in governance practices, provides training for stakeholders, promotes dark data awareness, ensures transparency, and builds a culture of understanding and protecting data and dark data across the organisation (Table 3.11

– CSF10). SF9 relies on a range of key practices (Table 3.11 - CSF4). These include actively engaging stakeholders to align with business needs and foster organizational buy-in, facilitating cross-functional collaboration to enhance diversity of perspectives, establishing dedicated data governance committees to resolve issues and align initiatives with organizational goals, regularly communicating governance policies and expectations to keep stakeholders informed and engaged, promoting collaboration across departments to ensure consistent management of dark data, leveraging cross-functional teams to bring varied expertise to governance efforts, engaging with regulatory bodies to maintain compliance with legal requirements, and establishing clear communication channels to ensure stakeholders understand and adhere to regulations. Collectively, these practices strengthen the organization's data governance culture and improve compliance and operational efficiency. Below are the key HDG communication channels (Rios, P, J., 2012) and HDG information flows (Achterbergh, J. and Vriens, D., 2002); (Preece, G., 2010) within SF9 (Communications among S3, S4 & S5) that are relevant to data governance and dark data systemic activities.

- **HDG Key Communication Channels within SF9**

- **HDG C12:** Relationship of SF3 with SF4
- **HDG C13:** SF3- SF4 Homeostat
- **HDG C14:** Relationship of SF4 and SF5
- **HDG C16:** Relationship of SF5 with SF3- SF4 Homeostat

- **HDG Key Information Flows within SF9**

- **HDG IF3: Organisational Goals generated by SF5:** The overarching governance support goals and objectives of the organisation are derived from strategic planning processes set by SF5. These goals provide unified direction and purpose for dark data governance across all other systems (SF1, SF3, SF4).
- **HDG IF22: Proposals for Innovation Made by SF4:** Suggestions for new ideas, products, or processes generated by SF4 and shared with SF5 and SF3 to drive dark data governance innovation and long-term adaptability to external requirements.
- **HDG IF29: Reviews by SF3 of Proposals for Innovation:** Evaluation of innovative dark data governance proposals by SF3, ensuring their feasibility and alignment with organisational goals. Information is shared with SF4 and SF5.
- **HDG IF30: Finalized Plans for Adaptation of Organisational Goals generated by SF3 and SF4:** SF3 and SF4 collaboration to approve dark data governance strategies and plans for adjusting organisational objectives, ensuring alignment with external

changes, and balancing present and future strategic goals. Information is shared with SF5.

- **HDG IF31: Regulatory Measures to Counter Imbalance Between SF3 and SF4 generated by SF5:** Steps defined by SF5 to address dark data governance conflicts or imbalances between SF3 and SF4, to maintain stability
- **HDG IF33: Norms for Balance Between SF3 and SF4 generated by SF5:** SF5 identification of dark data governance standards for maintaining equilibrium between SF3 and SF4, ensuring coordinated actions to balance present and future goals
- **HDG IF34: Actual Imbalance Between SF3 and SF4 generated by SF5:** SF5 identification of dark data governance current state of imbalance between SF3 and SF4 and determining areas needing attention.
- **HDG IF35: Causes of Imbalance Between SF3 and SF4 generated by SF5:** SF5 identification of Reasons for existing imbalances between SF3 and SF4 and understanding their causes.
- **HDG IF36: Experiences with IF31 generated by SF5:** SF5 identification of insights gained from implementing measures to balance SF3 and SF4, improving future responses.

Given the above, the ability of an organisation to adapt to environmental changes and learn from experiences is crucial for its long-term viability. This involves double-loop learning, where adjustments are made based on feedback, and underlying policies and goals are revised. The variety loop between SF3 and SF4 balances present and future orientations through strategic decision-making, monitored by SF5 for cohesion and alignment with organisational values and purpose. The metasystem comprising SF3, SF4, and SF5 ensures balanced data governance decision-making, maintaining homeostasis by integrating internal and external perspectives. Key HDG Communication channels (C12, C13, C14, C16) and key HDG information flows (IF3, IF22, IF29, IF30, IF31, IF33, IF34, IF35, IF36) facilitate coordination and innovation in data governance and dark data handling activities. This supports the achievement of operational and organisational goals.

4.4.2.11 Holistic Dark Data Governance Systemic Function (SF10): Communication channels and Algedonic channel

Effective communication channels are crucial for transmitting information between different sub-systems. This includes both vertical communication (between different hierarchical levels) and horizontal communication (across the same level). Feedback loops are essential for

ensuring that information flows back to the relevant units for continuous learning and adaptation about data governance and dark data handling. The key VSM communication channels and information flows must be established for the viability of a system in an organisation ([Rios, P., J., 2012](#)). SF10 includes defining, deploying and sustaining the systemic functions across the communication channels and information flows among all systems SF1, SF2, SF3, SF4, and SF5, to manage dark data risks requiring attention by all systems ([Beer, S., 1979](#)), ([Beer, S., 1981](#)). However, in case of crisis and high risks related to dark data (e.g. security breach) that threaten the organisation, immediate attention is required from the metasytem. The VSM algedonic channel raises alarms to trigger interventions outside normal regulatory channels. It includes activities that transfer signals from SF1 to SF5 directly, to manage dark data risks requiring immediate attention from the metasytem ([Beer, S., 1979](#)), ([Beer, S., 1985](#)), ([Lowe, D., Espinosa, A. and Yearworth, M., 2020](#)).

Given the above, Effective communication channels are essential for transmitting information between sub-systems, both vertically and horizontally, and for ensuring feedback loops that support continuous learning and adaptation in data governance and dark data handling. Key HDG communication channels and information flows must be established across all systems (SF1-SF5) to maintain viability and manage dark data risks through data governance systemic functions. In crises, the HDG algedonic channel triggers immediate interventions from the metasytem, ensuring rapid response to situations with high dark data risks such as security breaches. This supports the achievement of operational and organisational goals.

4.4.2.12 Holistic Dark Data Governance Transduction and Integration of all Systems - Common Data Governance Knowledge Systemic Function (SF11)

All sub-systems (SF1 to SF5) must be integrated and work cohesively as part of a larger whole. This integration ensures that the organisation functions effectively as a unified system, rather than as isolated parts ([Davies, J., 2002](#)) by defining, deploying and sustaining transduction and having a common dark data governance knowledge. Transduction is the systemic function of having a shared language (e.g. Metadata) across all systems (SF1, SF2, SF3, SF4, and SF5), related to data and dark data types. This is crucial to improve shared understanding between business and data stakeholders ([Khatri, V. and Brown, C., 2010](#)), ([Abraham, R., Schneider, J. and Brocke, v, J., 2019](#)), ([Otto, B., 2011](#)), ([Preston, D. and Karahanna, E., 2009](#)). This creates common cultural knowledge and reduces possible distortion and mitigates potential dark data risks/threats in communication between different stakeholders([Reynolds, M. and Holwell, S., 2010](#)),([Arghand, A., A., 2022](#)) – even within data stakeholders themselves and across all

communication channels to ensure viability([Beer, S., 1985](#)),([Huygh, T. and Haes, D, S., 2018](#)). Also, it creates a common understanding of organisational (data governance) culture and its impact on business operations and performance ([Preece, R, G., 2010](#)). SF11 manages metadata effectively, establishes standardized data definitions, fosters a shared understanding across the organisation, ensuring consistency and reducing misinterpretation for common understanding (Table 3.11 – CSF9). Examples of the metadata systemic function are the definitions of data types needed by the organisation and the definition of dark data types. Below is an example of key dark data types ([Hand, J, D., 2020](#)) – (described in Appendix A):

- DD-Type 1: Data We Know Are Missing
- DD-Type 2: Data We Don't Know Are Missing
- DD-Type 3: Choosing Just Some Cases
- DD-Type 4: Self-Selection
- DD-Type 5: Missing What Matters
- DD-Type 6: Data Which Might Have Been
- DD-Type 7: Changes with Time
- DD-Type 8: Definitions of Data
- DD-Type 9: Summaries of Data
- DD-Type 10: Measurement Error and Uncertainty
- DD-Type 11: Feedback and Gaming
- DD-Type 12: Information Asymmetry
- DD-Type 13: Intentionally Darkened Data
- DD-Type 14: Fabricated and Synthetic Data
- DD-Type 15: Extrapolating Beyond Your Data

Given the above, all sub-systems (SF1 to SF5) must be integrated and function cohesively to ensure the organisation operates as a unified governance system, rather than isolated parts. SF11 facilitates the integration among all systems through transduction, which involves having a shared language (metadata) across all systems related to data and dark data types. Such shared understanding improves communication between business and data stakeholders, creating common data governance knowledge and reducing potential dark data risks across the organisation. This also enhances organisational data governance culture, impacting business operations and supporting the achievement of operational and organisational goals.

The proposed model key systemic functions are summarised in Table 4.4 below.

HDG - Systemic Dimensions / Functions (SFs)) within the Organisational VSM Context	
VSM System-in-Focus (Organisational Level) and HDG Subsystems (SFs)	
1.	VSM Operational Units (S1: implementation) - HDG Support Systemic Functions (SF1) S1 delivers the products or services, with requisite variety to deal with their environment(s) and (SF1) complies with the Data Governance Supporting Systemic Functions (e.g. policies, guidelines) that are integrated with IT Governance and Corporate Governance Systemic Functions. This supports the achievement of operational and organisational goals (As described in Section 4.4.2.1 and Section 4.3)
2.	Co-ordination / Harmonization (S2) - HDG Co-ordination Systemic Functions (SF2): SF2 focuses on data governance systemic functions in integration with IT governance systemic functions within S2 that support the coordination of S1 operational activities. It handles oscillations from interactions between viable systems regarding digital data requirements and dark data risks, promoting synergies through cooperation. SF2 mechanisms, such as guidelines, procedures, and policies, ensure operational units work harmoniously. These mechanisms are viewed by S1 as supportive rather than obligatory since they are crucial to the achievement of operational and organisational goals (As described in Section 4.4.2.2 and Section 4.3)
3.	Control (Cohesion and Autonomy: S3) – HDG Control Systemic Functions (SF3) SF3 data governance systemic activities within S3 in integration with IT governance support the balance between self-regulation (Autonomy) for each of the operational units in S1 and their synergies (Cohesion) amongst them for improved organisational performance and achievement of operational and organisational goals. This includes data governance compliance management, performance management, legal and regulatory adherence, resource allocation, accountability, and policies for data

	governance domains (Data Architecture, Data Quality, Metadata, Data Security, Reference & Master Data, Data Warehousing/Business Intelligence/Artificial Intelligence, Data Modelling & Design, Document & Content Management, Data Storage & Infrastructure/Operation, Data Integration & Interoperability). (As described in Section 4.4.2.3 and Section 4.3)
4.	Audit (S3*) – HDG Audit and Compliance Systemic Functions (SF3*) SF3* within S3 includes data governance auditing functions that enable SF3 within S3 to gather information about dark data challenges and governance operations from S1 units. Key communication channels involve auditing and compliance coordination between S3, S3*, and S1 units. They focus on auditing and compliance evaluations to ensure accuracy and adherence to data governance standards, with results shared for corrective actions. This is to support the achievement of operational and organisational goals. (As described in Section 4.4.2.4 and Section 4.3)
5.	Intelligence / Adaptation (S4)- HDG Intelligence Systemic Functions (SF4) SF4 Making sense of environmental changes such as constraints and opportunities related to data needed by organisations and potentially encountering dark data that could threaten organisational viability. This shapes data governance strategy and long-term orientated tasks (e.g. research and development, market research, corporate planning) to support adaptability and the achievement of the organisation's long-term goals. (As described in Section 4.4.2.5 and Section 4.3)
6.	Policy (Identity and Closure - S5) – HDG Policy Systemic Functions (SF5) SF5 within S5 is the ultimate decision-making within a recursion of the viable system thereby providing logical closure to it. SF5 supports creating the corporate identity to provide consistent dark data governance systemic functions for business operations. SF5 sets the system's overall data governance direction, policies, values, and purpose and monitors the feedback loop between current (SF3) and future (SF4) data governance systemic functions. This ensures the balance between internal and external perspectives and supports the achievement of present operational and long-term organisational goals. (As described in Section 4.4.2.6 and Section 4.3)

HDG Subsystems (SFs) Interactions (Variety Loops) within the VSM System-in-Focus	
7.	Recursivity – Integration of Recursive HDG Systemic Functions at different levels of recursions (SF6) All data governance systemic functions at different levels of recursions are integrated to ensure viability and support the achievement of operational and organisational embedded goals. SF6 integrated systemic functions control data assets and their related digital activities including counteracting dark data risks at different levels of recursions. To develop a model of data governance that provides a holistic corporate context, this research adopts the corporation as the specific unit of analysis. As such, interactions with other different levels of recursions are outside the scope of this study. Future research can be conducted to study this systemic function and its integration across different levels of recursion. (As described in Section 4.4.2.7 and Section 4.3)
8.	HDG Requisite Variety in Response to the Environment - Systemic Functions (SF7) The dark data governance system must possess adequate internal variety to effectively govern the data assets and dark data risk handling in response to external digital disruptions and new data regulations, thereby establishing the requisite variety needed. Detecting and responding to dark data threats and opportunities is crucial to support the organisation's viability. This enables the organisation to remain agile and responsive to environmental changes. The VSM system-in-focus communicates with its environment through SF1 with its embedded viable systems and through SF4 with the total environment. These communications involve both short-term and long-term data governance activities focused on identifying and responding to data governance present and anticipated requirements and dark data threats within the system's environment to achieve organisational goals. (As described in Section 4.4.2.8 and Section 4.3)
9.	HDG Balance of Autonomy and Control – Inter-Operational Management Systemic Functions (SF8) This includes communications among SF1, SF2, and SF3. To ensure effective and responsive operational units (S1), sufficient autonomy is balanced with control within S1 through SF1 data governance support activities, SF2 data governance coordination, and SF3 data governance control systemic functions. This enhances decision-making

	through self-regulation and synergy and supports the achievement of operational and organisational goals. (As described in Section 4.4.2.9 and Section 4.3)
10.	HDG Metasystem Adaptability, Learning, and Change Management Systemic Functions (SF9) The metasystem comprising SF3, SF4, and SF5 provides the organisation with data governance decision-making capabilities. It balances present and future orientations and internal and external perspectives to maintain homeostasis regarding data governance and dark data handling. Key communication channels and information flows facilitate coordination and innovation in data governance and dark data handling activities. This supports the achievement of operational and organisational goals. (As described in Section 4.4.2.10)
11.	HDG Communication channels and Algedonic channel Systemic Functions (SF10) Key VSM communication channels and information flows must be established across all systems (S1-S5) to maintain viability and manage dark data risks through data governance systemic functions (SF1-SF5 and their integration). In crises, the VSM algedonic channel triggers immediate interventions from the metasystem, ensuring rapid response to situations with high dark data risks such as security breaches. This supports the achievement of operational and organisational goals. (As described in Section 4.4.2.11 and Section 4.3)
12.	HDG Transduction and Integration of all Systems - Common Data Governance Knowledge Systemic Functions (SF11) all sub-systems (S1 to S5) must be integrated and function cohesively to ensure the organisation operates as a unified system, rather than isolated parts. SF11 facilitates the integration among all systems through transduction, which involves having a shared language (metadata, e.g. dark data types, data types) across all systems related to data and dark data types. Such shared understanding improves communication between business and data stakeholders, creating common data governance knowledge and reducing potential dark data risks across the organisation. This also enhances organisational data governance culture, impacting business operations and supporting the achievement of operational and organisational goals. (As described in Section 4.4.2.12 and Section 4.3)

Table 4. 4 The Key Systemic Functions of a Holistic Data Governance (HDG)

4.5 Definitions of a Holistic Model for Dark Data Governance

As illustrated earlier in Chapter One, there is currently no agreed-upon definition for a holistic dark data governance framework within the literature. In order to determine what dark data governance is, chapter 1 of this study referred to some different definitions offered in the literature. However, a holistic framework to implement a dark data governance model is even harder to define because the area is both novel and constantly evolving. This study will adopt the context of cybernetics and Viable System Model (VSM) theories to examine dark data governance. Dark data governance focuses on how viable organisations use communications (data and information), and control actions to steer toward and maintain their goals while counteracting various dark data risks. To govern dark data effectively, this study conceptualizes the organisation through the Viable System Model (VSM), which assumes that organisations are inherently capable of achieving viability. Holistic dark data governance is integral to the overall systemic viability of the organisation. Consequently, to maintain consistency in this research, it is crucial to propose comprehensive definitions for a holistic model of dark data governance, holistic data governance, and dark data. These novel definitions are presented as follows:

- **Holistic Dark Data Governance** refers to the systemic functions of communication and data control aimed at mitigating the risks posed by dark data. It augments organisational viability by improving decision-making, fostering cohesion, enhancing adaptability, and generating business value. This supports the achievement of organizational operational and strategic goals.
- **Dark Data**, within the framework of the organisational Viable System Model (VSM), dark data is viewed as disturbances or risks that have the potential to disrupt organisational processes. Such disruptions can result in significant, and sometimes disastrous, consequences, jeopardizing the organisation's viability, purpose, and ability to achieve its goals.

These definitions will serve as the foundation for understanding holistic dark data governance and holistic data governance throughout the remainder of this study, particularly in relation to mitigating dark data risks.

4.5.1. Aim of the Model

This model aims to provide a methodology to help organisations understand the processes involved in conceptualizing a holistic dark data governance framework. This framework is

situated within the context of an organisation as a viable complex system, aiming to counteract the adverse consequences of dark data. Ultimately, it supports organisational viability and the achievement of operational and strategic objectives.

4.5.2. Analysis of Existing Data Governance

Given the diverse range of existing governance and data governance frameworks, and the critical systemic role of dark data governance described in this chapter, this research examined current frameworks in comparison to holistic viable systemic functions to support the development of a new model. This section presents a comparison of different governance frameworks against the key systemic functions of the Viable Systems Model. VSM is utilized to diagnose the completeness and coherence of governance systems. Beer's Viable Systems Model is a comprehensive framework designed to ensure the viability and effectiveness of organisations. The model emphasizes the following key viable systemic functions and qualities (details in Section 4.3.1) that are crucial for assessing support of governance models to organisational viability:

- S1: Operational Units
- S2: Coordination
- S3: Control
- S3*: Audit
- S4: Intelligence
- S5: Identity and Policy
- Requisite Variety
- Communication Channels
- Adaptability and Learning
- Balance of Autonomy and Control
- Integration of Sub-Systems
- Recursivity
- Transduction
- Algedonic Channels

By employing these qualities of VSM for assessment, one can determine the strengths and weaknesses of different governance models and how well they support the viability and effectiveness of an organisation.

Appendix J presents a comparative analysis of the following key governance models against the key qualities of Beer's Viable Systems Model, as detailed in Appendices J.1 and J.2:

- Young's Feedback Model (Young, D., 1996)
- Jessop's Coordination Model (Jessop, B., 1998)

- Rosenau's Comprehensive Model (Rosenau, N. J., 1992)
- Carver's Policy Governance Model (Carver, J., 1997)
- Charkham's Accountability Model (Charkham, J., 1994)
- Kay et al.'s Trusteeship Model (Kay, J. and Silbertson, A., 1995)
- Designing Data Governance (Khatari, V. and Brown, C., 2010),
- A Morphology of the Organisation of Data Governance (Otto, B., 2011),
- One Size Does Not Fit All: A Contingency Approach to Data Governance (Weber, K., Otto, B. and Osterle, H., 2009),
- Dark Data Management as Frontier of Information Governance (Ajis, M, F, A. and Baharin, H, S., 2019),
- Using the Viable System Model to Study IT Governance Dynamics (Huygh, T. and Haes, D, S., 2018))

Appendix K provides a comparison of the key industry governance models against the key qualities of VSM:

- COBIT (Control Objectives for Information and Related Technologies) ISACA, 2012
- DAMA-DMBOK (Data Management Body of Knowledge): DAMA International, 2017
- ISO/IEC 38500 (Corporate Governance of Information Technology): ISO, 2015.
- GDPR (General Data Protection Regulation): European Union, 2016
- CDMC (Cloud Data Management Capabilities): EDM Council, 2021

Each model has strengths and weaknesses in addressing these qualities, which helps in understanding the extent to which they support organisational viability and effectiveness.

Each model presented in Appendices J and K has strengths and weaknesses in addressing the key qualities of the Viable Systems Model, which helps in understanding the extent to which they support organisational viability and effectiveness. The evaluation reveals that although these models address various aspects of data governance effectively, they generally lack detailed mechanisms for Recursivity, Transduction, Algedonic Channels, and comprehensive holistic data governance as defined in Beer's Viable System Model. In contrast, the VSM framework offers a robust holistic context, ensuring coherence and adaptability through detailed communication, feedback, and systemic integration mechanisms. Consequently, none of the existing frameworks are entirely suitable for holistic data governance to counteract dark data and achieve organisational goals. The VSM provides a more comprehensive and integrated

approach to data governance, addressing the shortcomings of the other models and offering a path towards greater organisational viability and effectiveness.

4.6. Conceptualization of the Holistic Dark Data Governance Model

The gap analysis identified several deficiencies in previous studies and proposed frameworks, as discussed in Section 3.5.2. Specifically, existing data governance frameworks in the literature did not account for the unique characteristics of dark data governance. To mitigate these gaps, it is essential to develop a novel, holistic data governance model for dark data. This proposed model addresses the identified deficiencies and aims to fulfil the holistic data governance requirements within the context of the organisational Viable System Model (VSM).

VSM provides an integrated framework for designing flexible, adaptable organisations that balance external and internal perspectives and long and short-term thinking to gain holistic cohesion while achieving the organisation's purpose. VSM describes organisations as a system regulating the processing of variety (data & information). In the context of the Viable System Model (VSM), viability as a value creation context refers to an organisation's ability to self-organise, meet environmental challenges, act autonomously, and independently shape its future.

According to the Viable System Model (VSM), viable systems can be understood in terms of a set of parts distributed across the system and metasystem. These parts, which include policy, future/planning, integration/control (and associated audit), coordination, and operations, are generic to all autonomous systems. There is a relationship between these parts that involves both communication and control. The VSM is a theoretical framework for organisations, used as a central component of various approaches to address organisational viability issues. It is a generic model applicable to any organisation under certain guidelines to maintain viability ([Yolles, M., 2006](#)). Some of the key propositions of VSM are as follows:

- **Viability and Stability:** Viability implies that the system must maintain stability under changing conditions. This study focuses on necessary changes to handle data and counteract dark data.
- **Systemic Focuses:** A viable system can be viewed in terms of multiple focuses, each seen as a system in its own right. This study considers data governance as a holistic subsystem within the VSM framework to handle data and counteract dark data to support viability.

- **Recursivity, Autonomy and Self-Organisation:** Viable systems are autonomous, self-organising, adaptive, and autopoietic. An autopoietic system produces and reproduces its own elements and structures (Recursivity).
- **Metasystem Association:** A system is associated with a metasystem that comprises S3, S4, and S5, acting as its “cognitive consciousness.” This metasystem ensures effective decision-making, adaptability, and continuous learning and improvement.
- **Generic Model for Communication and Control:** VSM is a generic organisational model that promotes communication and control principles to maintain viability
- **Subsystems:** VSM proposes that any organisation conceptualized as a viable system can be represented as a set of five generic, interrelated subsystems: S1 (Operations/ Implementation), S2 (Coordination/ Harmonization), S3 (Integration/ Control), S4 (Future/ Planning), and S5 (Policy)
- **System Behaviour:** The behaviour of a system is defined by key operations that enable the organisation to achieve its objectives.
- **Variety:** The variety of a system refers to the number of possible states it can exhibit. Requisite variety is the necessary variety a system must have to deal with environmental variety. Variety can be managed by altering the form or behaviour of the organisation.

The Viable System Model (VSM) emphasizes that viability requires stability under changing conditions, necessitating systemic functions to handle data and counteract dark data. These systemic functions enable business value and consequently support achieving organisational goals (recursive goals). VSM views systems in terms of multiple focuses, treating data governance as a holistic subsystem to support viability. Viable systems are autonomous, self-organising, adaptive, and autopoietic, producing and reproducing their own elements and structures (Recursivity). The metasystem, comprising S3, S4, and S5, acts as the system’s cognitive consciousness, ensuring effective decision-making, adaptability, and continuous improvement. VSM promotes communication and control principles through five interrelated subsystems (S1, S2, S3, S4, and S5) to maintain system viability and achieve organisational goals by managing variety. This study proposed the corresponding interrelated HDG systemic functions within each subsystem as SF1 (HDG support to Operations/Implementation), SF2 (HDG Coordination/Harmonization), SF3 and SF3* (HDG Integration/Control and Audit/Compliance), SF4 (HDG Intelligence/Future Planning), and SF5 (HDG Policy within Organisational Identity). This study also proposed key HDG variety loops (SF6, SF7, SF8, SF9, SF10, and SF11) to support the viability of the organisation and the achievement of its goals. The HDG Model (HDGM) and its systemic functions from SF1 to SF5 are illustrated in

Figure 4.6 And the HDGM and its Systemic Functions from SF6 to SF11 are illustrated in Figure 4.7.

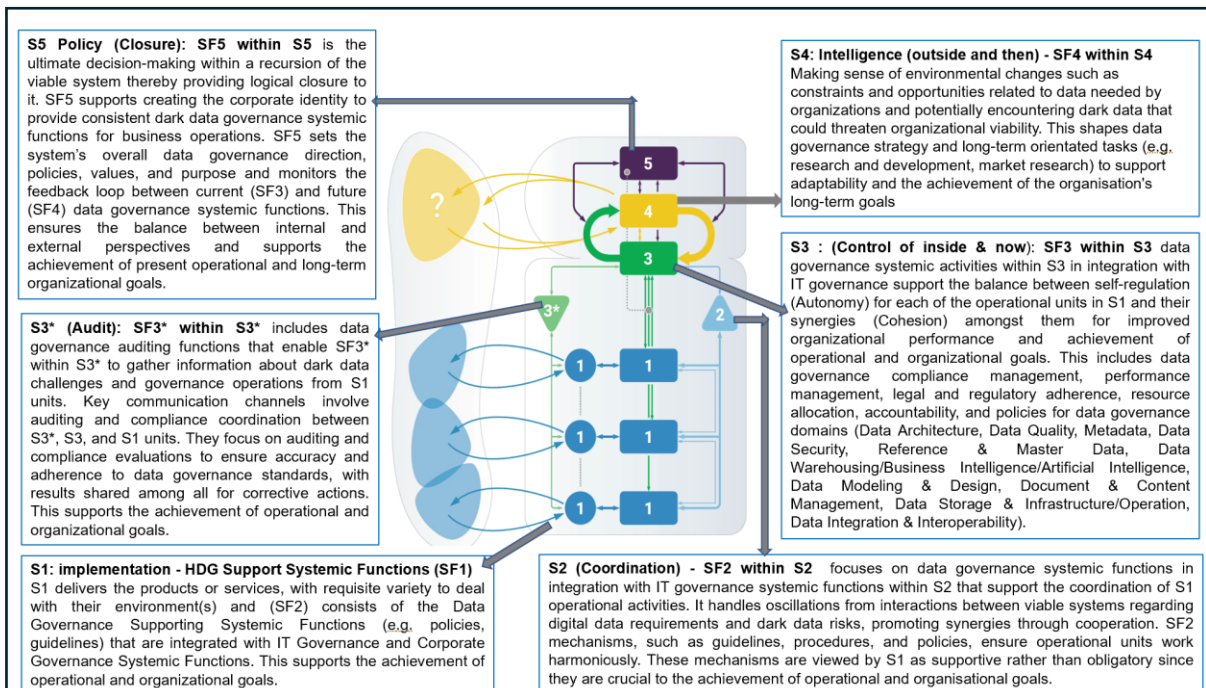


Figure 4. 6 HDGM Systemic Functions SF1 to SF5 within Organisational VSM Context

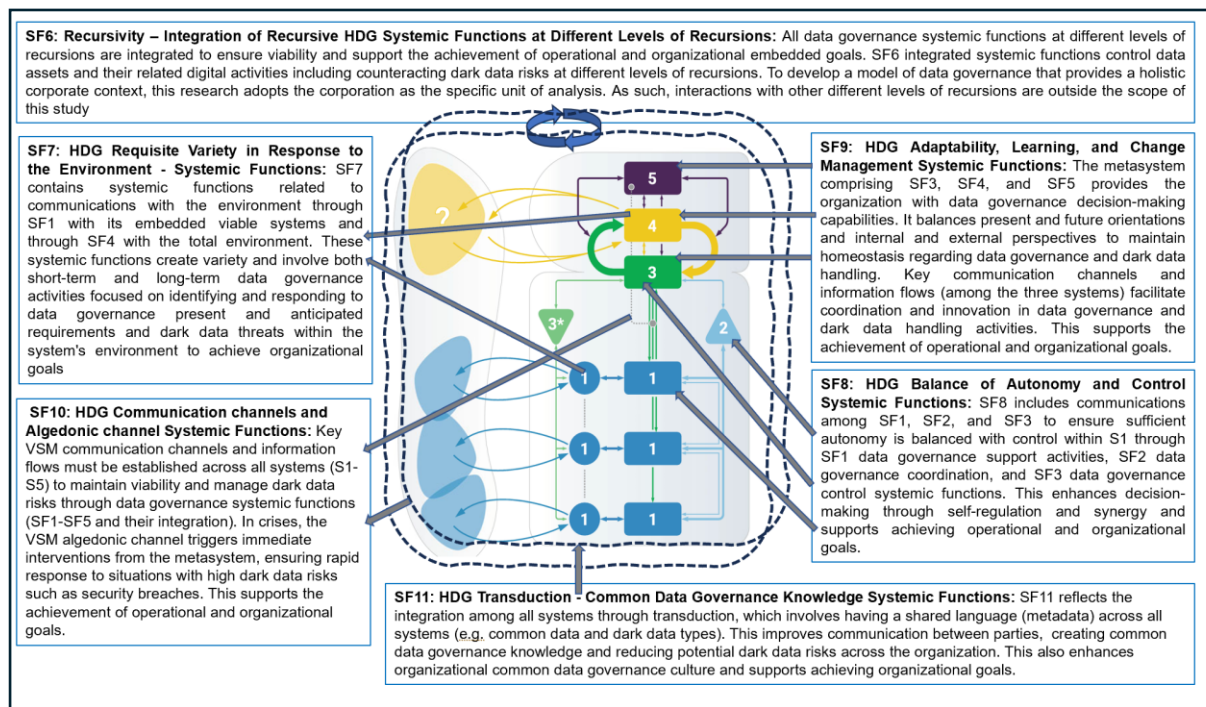


Figure 4. 7 HDGM Systemic Functions SF6 to SF11 within Organisational VSM Context

4.7. Methodology to Identify, Deploy, and Sustain the Proposed Model

The generality of the VSM makes it a powerful conceptual tool for both organisational diagnosis and design, independent of the specific features of the organisations under study, such as type of activity, size, location, products, markets, technology, and the like. To conceptualize the detailed holistic data governance model (HDGM) , this study combined and extended the following three methodologies that are described in Sections 4.7.1, 4.7.2, and 4.7.3 taking in consideration the literature compiled in Chapter 3 and Sections 4.3 and 4.4.2 of this chapter.

4.7.1 Performative Process Description of a VSM Epistemology

However, the cognitive accessibility of the VSM presents a significant barrier to its application with non-expert stakeholders ([Lowe, D., Espinosa, A. and Yearworth, M., 2020](#)). Consequently, a set of constitutive rules was proposed (Table 4.5) in order to make rigorous use of VSM theory ([Lowe, D., Espinosa, A. and Yearworth, M., 2020](#)). These rules fill in the gaps in the understanding between literature and practice. Also, they guide practitioners in their application of the VSM and account for the variety of VSM practices.

Principle	Description
Aiming to Bring About Improvements	The aim of using the VSM as a Problem Structuring Method (PSM) is to guide interventions and bring about improvements in problematic situations. While definitive solutions may be sought, improvement is the primary goal.
Using Models as Learning Devices	VSM-guided interventions use models to structure debates, enabling stakeholders to learn from each other about how organisations can improve their handling of complex situations.
Making No Assumption of Objective Viewpoints or Shared Worldviews	Recognize that different stakeholders bring various perspectives and may not share the same worldview. This diversity affects how content is elicited, managed, and implemented.
Tailoring Application to Practical Situations	The VSM provides a robust framework for complex situations, but each situation is unique. Tailor the application of VSM through conscious thought, balancing rigor and relevance.
Using Methods and Techniques Creatively to Examine the Problematic Situation	Match the approach to the needs of the complex situation by blending several specific methods and appreciating each method's respective strengths and weaknesses.

Principle	Description
Extracting Methodological Lessons Through Reflection	The use of VSM as PSM should yield research findings in addition to improving the problematic situation. These findings are typically methodological, relating to the intervention process rather than the problem itself, which will vary in every case.
Studying organisational interactions using VSM distinctions and principles, as an explicit epistemology to identify necessary interventions	If the Viable System Model (VSM) is to be used as a Problem Structuring Method (PSM) for studying organisational interactions and identifying interventions, the PSM must adhere to the distinctions and principles established by the VSM. Ensuring that the implemented PSM aligns with the underpinning theory is crucial for the validity of results and the long-term credibility of both the VSM and PSMs in general. This adherence underscores their rigorous nature as methodologies for complex problem-solving

Table 4. 5 Constitutive Rules for an Interpretive VSM Methodology

The aim of using the VSM as a PSM is to bring about improvements in problematic situations, recognizing that seeking definitive solutions is often impractical. VSM-guided interventions use models to structure debates, facilitating stakeholder learning and organisational improvement. It is crucial to acknowledge that different stakeholders bring diverse perspectives and worldviews, impacting content elicitation and process implementation. The VSM must be tailored to each unique situation, balancing rigor and relevance. Creative blending of methods is essential to address complex situations, leveraging their respective strengths and weaknesses. Reflective use of the VSM should yield methodological insights beyond situational improvements.

Taking into consideration the above constitutive rules where VSM is considered a Problem Structuring Method (PSM), a comprehensive performative process description of a VSM epistemology was developed (Lowe, D., Espinosa, A. and Yearworth, M., 2020), identifying 14 process elements grouped into three processes of inquiry (Table 4.6):

	Sub-Process
Defining the system in focus – concepts described in Sections 4.3.1	1. Organisational Identity – Establishing a purpose for the organisation (products or services), its stakeholders, and its boundaries.
	2. Levels of Recursive Organisation – Identifying the sub-organisations directly responsible for implementing core products or services and the larger system of which the system in focus is part.

	Sub-Process
Identifying & assessing the sub-systems within the system-in-focus	3. Operational Units (S1) – Delivering the products or services, with requisite variety to deal with their environment(s).
	4. Harmonisation (S2) – Preventing recurrent conflicts amongst primary units, by providing shared values, languages, standards, and protocols for information, communications, and processes.
	5. Self-Regulation and Synergies (S3) – Supporting self-regulation for each of the operational units and realizing synergies amongst them for improved organisational performance.
	6. Monitoring (S3*) – Informal monitoring of operational performance.
	7. Adaptation (S4) – Making sense of environmental changes (constraints and opportunities), to shape strategy and long-term orientation.
	8. Identity and Closure (S5) – Creating corporate identity, ethos, and policies to provide a consistent framework for operations.
Identifying & assessing the interactions within the system-in-focus	9. Resource Bargaining (S3–S1) – Negotiating expected results, and matching resources for each of the operational units.
	10. Inter-operational Management (S1–S2–S3) – Managing operational complexity and enabling effective decision-making.
	11. Strategy Development Processes (S4–S3) – Combining internal and external perspectives on feasible and desirable future developments, to support strategy development for the organisation.
	12. Maintaining Balance (S5–S4–S3) – Balancing between present and future orientations and between internal and external perspectives in order to keep the organisation in homeostatic balance with its niche.
	13. Recursive Governance – Ensuring that each embedded organisation operates as a viable system itself (with appropriate autonomy to self-govern).
	14. Algedonic Signals – Raising alarms to trigger interventions outside of the normal regulatory channels.

Table 4. 6 Performative process description of VSM epistemology.

4.7.2 The Methodology of Diagnosis and Design by VSM

The Viable System Model (VSM) methodology (Figure 4.8, and Table 4.7) focuses on diagnosing and improving organisational viability through cybernetic principles. It involves three stages: system identification, system diagnosis, and addressing other VSM requirements. These stages help establish organisational purpose, analyse subsystems (S1-S5), and

implement corrective actions to ensure stability and adaptability. The methodology integrates ontological, epistemological, and axiological perspectives to enhance organisational structure and functioning.

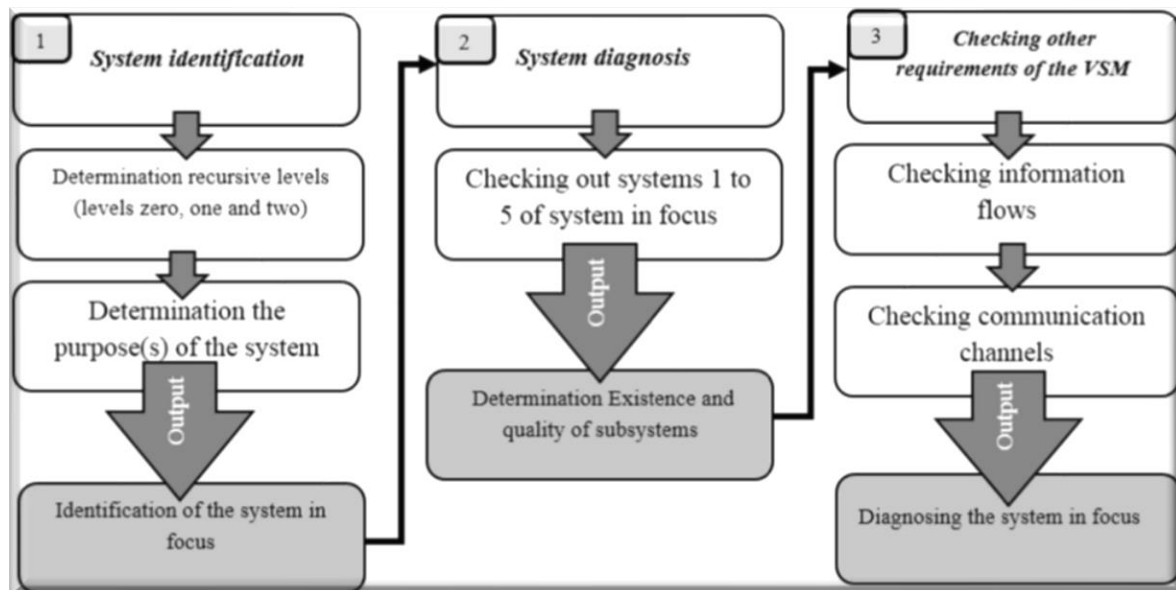


Figure 4. 8 The Methodology of Diagnosis and Design by VSM (Rezaee, Z. et al., 2018)

Stage	Description
System Identification	Establishing the purpose and boundaries of the system, identifying primary and supporting functions, and determining recursive levels – described in Sections 4.3.1, 4.3.2 of this Chapter Output: System-in-Focus
System Diagnosis	Checking out Systems 1 to 5 of System-in-Focus Output: Existence and quality of Systems (Quality vs. Criteria in Appendix L)
Other Requirements	Checking Communication Channels (C1-C17) – described in Section 4.3.4 of this Chapter Checking Key VSM Information Flows (IF1 to IF38) – described in Section 4.3.5 of this Chapter Output: Diagnosing System-in-focus

Table 4. 7 The Methodology of Diagnosis and Design by VSM

4.7.3 Cycle of the VSM Methodology to diagnose an organisation

The Viable System Model (VSM) methodology follows a structured cycle that includes several steps to diagnose and correct organisational issues, ensuring stability and viability. The process is represented in a cyclical diagram, emphasizing continuous improvement and adaptation

(Yolles, M., 2006, Beer, S., 1979, and Beer, S., 1985). The VSM methodology involves a continuous loop of diagnosing, defining, and correcting systemic issues. This process is designed to ensure the organisation can adapt to changes and maintain viability. The cycle includes specifying the system's purpose, diagnosing both the system and metasytem, defining the system's components and viable parts, and implementing corrective actions based on evaluation against predefined measures. Stakeholder participation and feedback are integral throughout the process to ensure alignment with organisational goals.

This diagram (Figure 4.9) represents the Viable System Model (VSM) methodology, illustrating the continuous cycle that includes the following steps to diagnose, define, and correct organisational issues to ensure stability and viability where the problem owner is consulted throughout the logical process of inquiry:

- **Conceptualization Phase:**

- **Identify Purpose (1):** Define the core purpose of the system, its goals, and objectives.
- **Determine System in Focus (2):** Establish the boundaries and scope of the system to be analysed.
- **Specify Viable Parts (3):** Identify all sub-systems and components that contribute to the system's viability.
- **Specify Whole (4):** Define how the identified parts integrate to form a coherent whole system.
- **Control:** Confirm the conceptualization steps with problem owners (Possible recursion may happen)

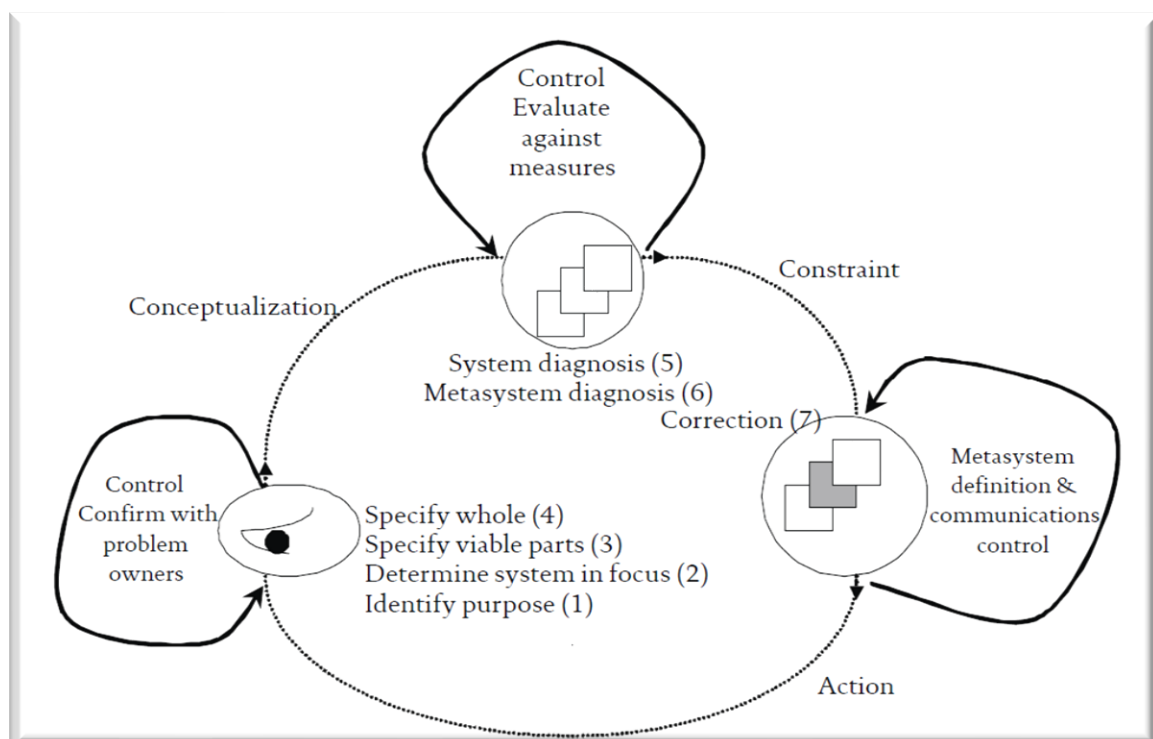
- **Action Phase:**

- **System Diagnosis (5):** Analyse the current state of the system to identify strengths, weaknesses, opportunities, and threats.
- **Metasystem Diagnosis (6):** Evaluate the metasytem, ensuring it supports the system's viability.
- **Control:** Define the metasytem and establish effective communication channels.

- **Constraint Phase:**

- **Correction (7):** Implement corrective actions based on the diagnostic findings.
- **Control:** Continuously evaluate the system's performance against predefined measures.

This structured approach ensures that the organisation continuously adapts and evolves, maintaining stability and achieving its strategic objectives despite changing external conditions.



Given the above, the following section describes the methodology proposed to deploy and sustain the proposed model (HDGM)

4.7.4 Methodology to identify, deploy, and sustain the HDGM

The need for a comprehensive data governance methodology arises from the increasingly complex and dynamic nature of organisational environments, where traditional approaches often fall short. The three methodologies discussed (Methodology 1. Performative Process Description of a VSM Epistemology, Methodology 2. the Methodology of Diagnosis and Design by VSM (Rezaee et al., 2018), and Methodology 3. the Cycle of the VSM Methodology) collectively provide a vital foundation for addressing this challenge. However, integrating their strengths into a holistic data governance framework can further enhance organisational adaptability, stability, and strategic alignment to ensure viability.

The Performative Process Description of a VSM Epistemology emphasizes using the VSM as a Problem Structuring Method (PSM) to guide interventions, improve problematic situations, and facilitate organisational learning through diverse stakeholder perspectives. This methodology highlights the importance of tailored application and methodological reflection, ensuring that the governance framework remains relevant and adaptive to specific organisational contexts. By leveraging these principles, a holistic data governance methodology can ensure continuous improvement and dynamic adaptation to emerging challenges related to dark data, especially fatal dark data risks. The proposed dark data governance enhanced the 14 process elements (within Methodology 1) by adding additional systemic governance functions (Information flows across the organisation: IF1 to IF38) that are covered only within Methodology 2. Information flows (IF1 to IF38) were incorporated within all dark data governance systemic functions as appropriate. This ensures a comprehensive understanding of organisational systemic governance functions, thereby enhancing the overall effectiveness and coherence of the governance framework. Also, the proposed methodology to deploy and enhance HDGM incorporates the unique aspect within Methodology 3 which is the continuous loop of diagnosing, defining, and correcting systemic issues to maintain organisational stability and viability. This cyclical approach, which emphasizes continuous improvement and stakeholder feedback, ensures that the governance framework remains aligned with organisational goals and responsive to dark data challenges. Incorporating this cyclical process into the proposed dark data governance methodology can foster a culture of ongoing evaluation and refinement, ensuring that governance practices evolve in tandem with organisational needs and external demands.

By synthesizing the strengths of these three methodologies, the proposed methodology to deploy and sustain the holistic data governance model can address the complexity and dynamism of modern organisational environments and ensure robust, adaptable, and strategically aligned governance practices. This integrated approach will provide a comprehensive, flexible, and reflective methodology, capable of managing data effectively and counteracting the risks associated with dark data, thus supporting long-term organisational viability and goal achievement.

The methodology to deploy and sustain HDGM is described in Table 4.8. and illustrated in Figure 4.10.

Systemic Phase 1: Identify the Organisational VSM System-in-focus and Contextualize/Deploy, and Sustain the Holistic Dark Data Governance Sub-System (HDGM) within the VSM Context		
1.	Organisational Identity / Purpose (VSM Context) and HDG Purpose within VSM Organisational Context	Determine the purpose of the organisation (products or services), its stakeholders, and its boundaries within the VSM context Define dark data governance purpose. Dark Data governance purpose for this study is to counteract dark data risks and create business value to support organisational viability and goal achievement. (As described in Section 4.4)
2.	Levels of Recursive Organisation and HDG Scope	Identify the sub-organisations directly responsible for implementing core products or services and the larger systems of which the System-in-Focus is part of (levels of recursion). Defines the HDG scope, counteract dark data risks, and create business value to support achievement of organisational goals. The System-in-focus for this study is at an organisational level. (As described in Section 4.4.1.)

Systemic Phase 2: Identify, Deploy, and Sustain the Holistic Dark Data Governance (HDG) Systemic Functions (SFs) within the Organisational VSM system-in-focus (Organisational Level)		
3.	HDG Systemic Functions (SF1) within Operational Units/ Implementation Units (S1)	HDG SF1 (within S1) encompasses the identification, deployment and sustainability of HDG policies, guidelines, and procedures, integrated with IT governance and Corporate Governance, to counteract dark data while providing the necessary data for implementing primary activities. The main purpose is to continuously support organisational viability and the achievement of operational goals. (As described in Section 4.4.2.1 and Section 4.3)
4.	HDG Co-ordination / Harmonisation (SF2) within S2	HDG SF2 (within S2) defines, deploys and sustains compliance with corporate dark data governance systemic functions (e.g. corporate policies, guidelines, standards, rules, and protocols) to prevent recurrent dark data governance conflicts and misalignment among primary units within S1. Deploy identified corrective actions and improvements as appropriate to support improved corporate harmonization continuously. (As described in Section 4.4.2.2 and Section 4.3)
5.	HDG Cohesion, Control, & Autonomy: (SF3) within S3	HDG SF3 (within S3) defines, deploys, and sustains corporate dark data governance systemic functions: HDG Corporate policies, HDG performance measurements, HDG compliance requirements, HDG resource requirements (e.g. Technology, Financials, competencies) requirements, and allocation of HDG resources to SF1. Corporate policies are developed for key data governance domains (Data Architecture, Data Quality, Metadata, Data Security, Reference & Master Data, Data Warehousing/Business Intelligence/Artificial Intelligence, Data Modelling & Design, Document & Content Management, Data Storage & Infrastructure/Operation, Data Integration & Interoperability)

		Sustainability is based on HDG's evolving requirements and gaps identified for holistic dark data governance. HDG SF3 supports the balance between self-regulation (Autonomy) for each operational unit in S1 and their synergies (Cohesion) amongst them for improved organisational performance and achievement of operational and organisational goals. (As described in Section 4.4.2.3 and Section 4.3)
6.	HDG Audit and Compliance (SF3*) within S3*	HDG SF3* within S3 is to identify, conduct, and sustain data governance auditing functions that enable SF3 within S3 to gather information about dark data challenges and governance operations from S1 units. Key communication channels involve auditing and compliance coordination between S3, S3*, and S1 units. They focus on auditing and compliance evaluations to ensure accuracy and adherence to holistic data governance standards, with results shared for corrective actions. This is to support the achievement of operational and organisational goals. (As described in Section 4.4.2.4 and Section 4.3)
7.	HDG Intelligence /Adaptation (SF4) within S4	HDG SF4 within S4 (e.g. HDG research and development, HDG market research, HDG corporate planning) makes sense of environmental changes such as constraints and opportunities related to data needed by the organisation and potentially encountering dark data that could threaten organisational viability. This identifies, deploys, and sustains holistic data governance strategy and long-term orientated tasks to support and improve the adaptability and the achievement of the organisation's long-term goals. (As described in Section 4.4.2.5 and Section 4.3)
8.	HDG Policy, Identity, and Closure (SF5) within S5	SF5 within S5 plays a crucial role in establishing, deploying, and sustaining the corporate integration of HDG policies to continuously ensure a consistent operational governance framework. SF5 within S5 is the ultimate dark data governance decision-making within a recursion of the viable system thereby providing logical closure to it. SF5 supports creating the corporate identity (S1) to provide consistent dark data governance systemic functions for business operations. SF5

		sets the system's overall data governance direction, policies, values, and purpose and monitors the feedback loop between current (SF3) and future (SF4) data governance systemic functions (in integration with corporate IT governance and corporate governance). This ensures the balance between internal and external perspectives and supports the achievement of present operational and long-term organisational goals. (As described in Section 4.4.2.6 and Section 4.3)
Systemic Phase 3: Identify, Deploy, and Sustain the Key Interactions (Variety loops /Feedback loops) among the Holistic Dark Data Governance Systemic Functions (HDG SFs) within the Organisational VSM system-in-focus		
9.	HDG Recursive Systemic Functions (SF6)	Recursivity ensures that each embedded organisation operates as a viable system itself (with appropriate autonomy to self-govern). All data governance systemic functions within and at different levels of recursions are integrated with other relevant governance domains to counteract dark data and support the achievement of operational and organisational embedded goals. The VSM is fractal in nature, meaning that each viable system, at any given level of recursion, can be modelled using exactly the same syntax and this is applied to SF6 Systemic functions at each level of recursion. SF6 integrated systemic functions handle required data assets and their related digital activities including counteracting dark data risks at different levels of recursions. To develop a model of data governance that provides a holistic corporate context, this research adopts the organisation as the specific unit of analysis. Accordingly, the model can be applied at any other level of recursion since it has the same structural context. Future research can be conducted to study this systemic function and its integration across different levels of recursion. (As described in Section 4.4.2.7 and Section 4.3)

10.	HDG Requisite Variety Systemic Function (SF7) (SF1-Environment) (SF4-Environment)	The dark data governance systemic functions (SF7) must possess adequate internal variety to effectively govern the data assets and dark data risk handling in response to external digital disruptions and new data governance functions (e.g. regulations), thereby establishing and sustaining the requisite variety needed. Detecting and responding to dark data threats and opportunities is crucial to support the organisation's viability. This enables the organisation to remain agile and responsive to environmental changes. The VSM system-in-focus communicates with its environment through SF1 with its embedded viable systems and through SF4 with the total environment. These communications involve both short-term and long-term data governance activities focused on identifying, deploying and responding to data governance present and anticipated requirements and dark data threats within the system's environment to achieve organisational goals (As described in Section 4.4.2.8 and Section 4.3)
11.	HDG Inter-operational Management (SF1–SF2–SF3) Systemic Functions – HDG SF8	This includes defining, deploying and sustaining the key communications among SF1, SF2, and SF3. To ensure effective and responsive operational units (S1), sufficient autonomy is balanced with control within S1 through SF1 data governance support activities, SF2 data governance coordination, and SF3 data governance control systemic functions. This enhances decision-making through self-regulation and synergy and supports achieving operational and organisational goals. (As described in Section 4.4.2.9 and Section 4.3)
12.	HDG Metasystem (SF3-SF4-SF5) Adaptability, Learning, and Change Management Systemic Functions (SF9)	The metasystem comprising SF3, SF4, and SF5 (within the S3, S4, and S5 corporate metasystem) provides the organisation with data governance decision-making capabilities. It balances present and future orientations and internal and external perspectives to maintain homeostasis regarding data governance and dark data handling. It defines, deploys and sustains the key communication channels and information flows within the metasystem to facilitate coordination, innovation, adaptability, learning, and change management in data governance and dark data handling

		activities. This supports the achievement of operational and organisational goals. (As described in Section 4.4.2.10 and Section 4.3)
13.	HDG Communication channels and Algedonic channel Systemic Functions (SF10)	This includes defining, deploying and sustaining the key VSM communication channels and information flows across all systemic functions (SF1-SF5) to maintain viability and manage dark data risks. In crises, the VSM algedonic channel (SF1-to SF5 directly) triggers immediate interventions (outside of the normal regulatory channels) from the metasytem, ensuring rapid response to situations with high dark data risks such as security breaches. This supports the achievement of operational and organisational goals. (As described in Section 4.4.2.11 and Section 4.3)
14.	HDG Transduction and Integration of all Systems - Common Data Governance Knowledge Systemic Functions (SF11)	It defines, deploys and sustains systemic functions (SF1 to SF5) integration to ensure that the organisation operates cohesively and as a unified system, rather than isolated parts. SF11 ensures integration among all data governance systemic functions through transduction, which involves having a shared language (metadata, e.g. dark data types, data types) across all systems related to data and dark data types. Such shared understanding improves communication between business and data stakeholders, creating common data governance knowledge and reducing potential dark data risks across the organisation. This also enhances organisational data governance culture, impacting business operations and supporting the achievement of operational and organisational goals. (As described in Section 4.4.2.12 and Section 4.3)

Table 4. 8 Methodology to Identify, Deploy, and Sustain HDGM

This continuous improvement approach, as illustrated in Figure 4.10, ensures that the organisation adapts to changes and dark data challenges, sustains stability, and achieves its operational and strategic objectives by integrating holistic robust dark data governance systemic functions with continuous improvements. This will be explained in detail in Chapter 5. This Chapter focuses on how to define, deploy, and sustain the Systemic functions (SF1 to

SF11) of the proposed Holistic Data Governance Model (HDGM) within the organisational VSM context.

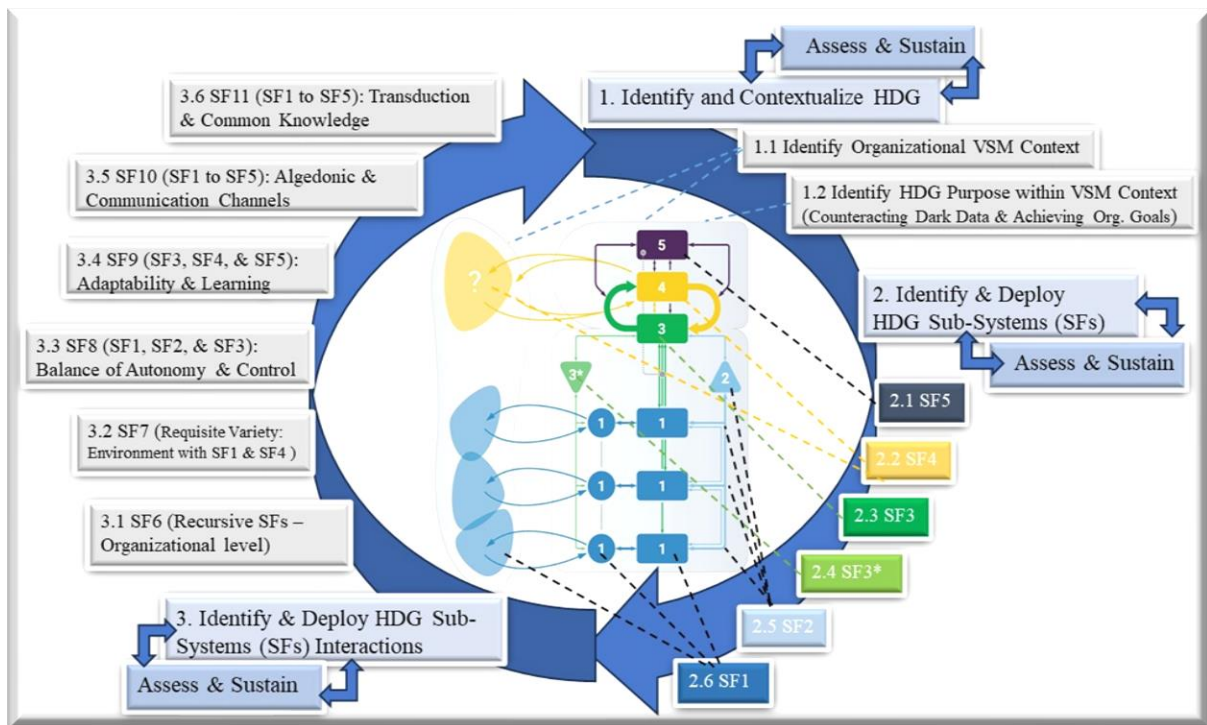


Figure 4. 10 Methodology to Identify, Deploy, and Sustain the HDGM

4.8. The Roadmap to Manage the Deployment and Sustainability of HDGM

The proposed holistic dark data governance model (HDGM) was developed based on three major phases (Section 4.7.4 and Table 4.8), each with important systemic functions. The roadmap for deploying and sustaining this model within organizations is outlined in Figure 4.11. This roadmap involves defining the Viable Systems Model system-in-focus and the Holistic Dark Data Governance Model context. It begins by determining the organizational purpose and dark data governance goals, followed by the identification of recursive organizational levels. The roadmap further encompasses the identification, deployment, and maintenance of dark data governance subsystems, including systemic functions (SF1) within operational units (S1) to effectively support the delivery of organizational products or services. Additionally, HDGM incorporates coordination (SF2) and control (SF3) mechanisms to prevent conflicts and ensure alignment with corporate dark data governance policies, as well as auditing functions (SF3*) to gather and evaluate relevant information to ensure compliance. Adaptation systemic functions (SF4) assess environmental changes and shape long-term dark data governance strategies, while policy, identity, and closure functions (SF5) maintain a

consistent corporate identity for dark data governance. The interactions among dark data governance systemic functions support overall organizational viability, with recursive systemic functions (SF6) and requisite variety (SF7) addressing both internal and external challenges related to dark data governance. Effective dark data governance inter-operational management (SF8), operational and strategic adaptability (SF8), risk mitigation communication channels (SF10), and integration of all systemic functions through common data governance knowledge (SF11) are also, essential for counteracting dark data, supporting organizational stability and achieving organizational goals.

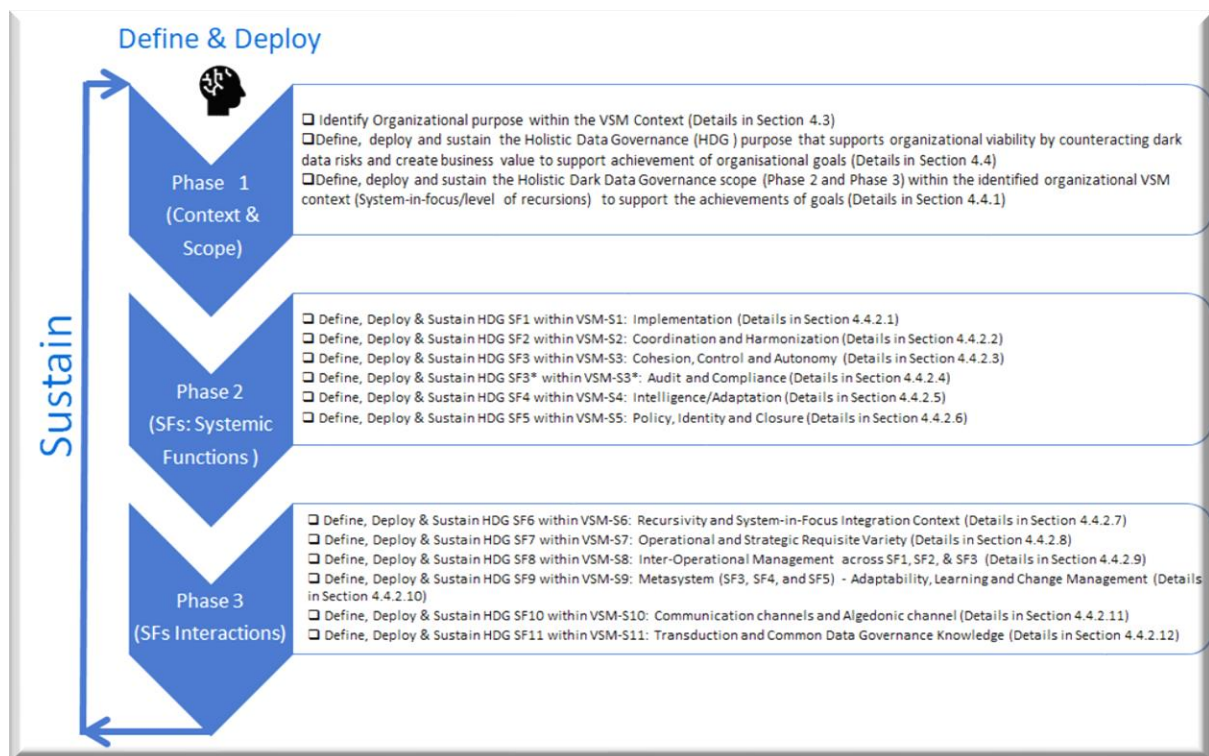


Figure 4. 11 Roadmap to Manage the Deployment and Sustainability of HDGM

This roadmap ensures that the organisation adapts to changes and mitigate dark data challenges, maintains stability, and achieves its operational and strategic objectives by integrating holistic, robust, and interconnected systemic functions for dark data governance. This roadmap focuses on defining, deploying and sustaining the Systemic functions of the proposed Holistic Dark Data Governance Model within the organisational Viable Systems Model context to continuously support the organisation's overall viability and effectiveness in addressing the complex challenges posed by dark data and in achieving its goals.

4.9. Chapter Summary

This chapter presents one of the core contributions of this thesis, i.e. a holistic model to deploy, assess, and sustain effective dark data governance systemic functions within the organisational VSM context. This chapter outlines the necessity for a comprehensive framework to address dark data within an organisational context. Current frameworks fail to align dynamically with business objectives or account for interconnectedness among governance components. The proposed model integrates the Viable System Model (VSM) and Critical Success Factors (CSFs) to establish a holistic data governance model that emphasizes continuous alignment with business goals and the proactive management of dark data risks. This model encompasses various systemic functions, including operational, coordination, control, intelligence, policy, recursion, requisite variety, and balance of autonomy and control for dark data governance within the VSM context. The chapter emphasizes organisational adaptability, continuous learning, and balancing autonomy and control to counteract dark data risks and ensure organisational viability and achievement of its goals. A methodology and a roadmap for implementing, deploying, and sustaining the model within the VSM context are outlined, focusing on defining the system-in-focus, deploying subsystems, and ensuring sustainability. This approach aims to enhance decision-making, manage dark data risks, and support organisational viability and stability.

Chapter 5: Holistic Dark Data Governance Maturity Model and Assessment Matrix

5.1. Introduction

As organisations carry out their operational and strategic activities, they accumulate substantial volumes of data. However, over time, a significant portion of this data is left unattended within the organisation's data repositories, without undergoing further analysis or processing, frequently due to constraints in financial, human, or temporal resources ([Weber, K., Otto, B. and Osterle, H., 2009](#)). Ambiguous policies governing the data lifecycle, encompassing the stages from data acquisition to disposal, contribute to the proliferation of dark data, with estimates suggesting that over 50% of organisational data remains unanalysed and underutilized as dark data ([Marus, P., 2018](#)). Although the dangers associated with dark data have been widely acknowledged, the rapid growth in large-scale data gathering and the advancing complexity of analytical tools like artificial intelligence and machine learning may be worsening these issues ([Hand, D., 2020](#)). The existing solutions for addressing dark data risks demonstrate feasible approaches, but they have failed to propose a comprehensive holistic dark data governance model that considers the organisational context at both the intra-organisational and inter-organisational levels. Until recently, holistic dark data governance has been predominantly informal, confined within specific data repositories, and lacking structured processes and organisation-wide support (Hand, J, D., 2020). This chapter builds upon the limitations of current approaches to data governance, which may not holistically address the risks posed by dark data. It extends the holistic model for dark data governance developed in Chapter 4 by proposing a maturity model and performance assessment matrix to evaluate the implementation of the holistic model within an organisation's systemic context. The aim is to provide organisations with instruments to evaluate the state of their comprehensive data governance practices and drive continuous enhancement towards the effective implementation of holistic dark data governance systemic functions within the organisational VSM framework. The systematic literature review in Chapter 3 revealed a gap in research on dark data governance models, linked to maturity and assessment matrices. While existing data governance maturity models are available, they do not adequately address the unique characteristics of dark data. This chapter aims to expand the research in this area and develop a novel approach to enable organisations to achieve effective and efficient dark data governance. Furthermore, this research seeks to augment the academic literature accessible to stakeholders interested in holistic dark data governance. It seeks to provide them with a

mechanism to elevate their holistic dark data governance systemic functions. The primary objectives of this research are to develop a new maturity model and assessment matrix specifically for dark data governance. It also provides a methodology and innovative approach to guide organisations in developing an enhanced roadmap for their holistic dark data governance. This allows them to attain a specified maturity level, which supports the achievement of their organisational objectives.

Maturity models have been extensively employed within the domain of Information Systems for an extensive period (Frick, N., 2012). The maturity approaches emerged initially within the domain of quality management and were subsequently adapted and applied in the field of information technology to support the management of software development processes (Crowston, K. and Qin, J., 2010). Maturity models serve as measurement frameworks that allow organisations to assess their capabilities and performance with respect to a specific domain or challenge (Blommerde, T. and Lynch, P., 2016). The existing literature indicates a prominent presence of diverse data governance maturity models, which reflects the substantial interest and engagement exhibited by industry stakeholders in this domain (Adler, S., 2007), (Nascio., 2009). Academic literature lacks comprehensive maturity models for holistic dark data governance, as developing such a model necessitates incorporating key features pertaining to the organisation's systemic context. Nonetheless, the existing data governance maturity models have failed to incorporate these critical elements. As a result, the current maturity models do not sufficiently address the research problem, as they neglect to consider holistic dark data governance within a systemic organisational context. The existing data governance maturity models lack the comprehensive coverage of best practices and dimensions required for effective holistic dark data governance, indicating a need for a more robust and inclusive maturity model in this domain. This chapter introduces a novel holistic dark data governance maturity model that comprehensively captures the diverse dimensions of the holistic dark data governance framework outlined in Chapter 4. These dimensions underpin an organisation's execution of the key holistic dark data governance systemic functions, which will also be outlined based on the maturity levels of the model. Additionally, an assessment matrix for the Holistic Dark Data Governance Maturity model will be developed, grounded in the HDGM maturity model. This assessment matrix will enable organisations to evaluate the current state of their holistic dark data governance practices, with the aim of guiding them towards the target state to support the achievement of their organisational objectives.

5.2. Findings from the Literature Review on Maturity Models

The utilization of maturity models has been widespread across information system domains. In order to fulfil the objective of developing a holistic dark data governance maturity model for this chapter, the research status of maturity models was investigated. The literature review guidelines proposed by Kitchenham and Charters were employed to identify and examine relevant maturity models (Kitchenham, B. and Charters, S., 2007). The researchers formulated five research questions to conduct a review of maturity model literature, with a particular focus on the research designs, research methods, and theoretical foundations underlying existing maturity models. Additionally, the maturity model domains and validation methods were considered in the review questions (Table 5.1).

Review Questions No.	Review question	Motivation
RQ1	What are the most common research designs applied?	This question investigates the predominant research designs employed in the development of maturity models.
RQ2	What are the most common research methods applied?	This question investigates the predominant research methods employed in the development of maturity models.
RQ3	What are the most common theoretical foundations to develop maturity models?	This question investigates the key theoretical underpinnings that guide the development of maturity models.
RQ4	How are the developed maturity models validated?	This question investigates the methods used to validate that maturity models are suitable for their intended purpose.
RQ5	In what domains is maturity model research applied?	This question investigates the breadth of application for the concept of maturity models across diverse domains.

Table 5. 1 Maturity Models Literature Review Questions

The literature review (described in Appendix M) findings are summarized as follows.

- (RQ1) Research Designs: The development of maturity models relies on a variety of research designs, including empirical research, design-oriented approaches, conceptual research, Design Science Research, case studies, action research, and grounded theory.

These designs allow researchers to create robust models that are both theoretically sound and practically relevant. Mixed methods are particularly useful, as they combine the strengths of qualitative and quantitative approaches, ensuring that maturity models are validated from multiple perspectives.

- (RQ2) Research Methods: The development of maturity models requires a combination of research methods that are both qualitative and quantitative. Common methods include concept development, workshops, focus groups, action research, the Delphi method, and qualitative and quantitative methods. Mixed methods are particularly effective in combining the strengths of both qualitative insights and quantitative validation, ensuring that the maturity model is both theoretically sound and practically applicable.
- (RQ3) Theoretical Foundations: The development of maturity models is grounded in several key theoretical foundations, each of which provides a unique perspective on how organisations progress and improve their capabilities. Capability maturity model theory offers a structured approach for measuring and improving performance, while concept construction ensures that models are grounded in established theory. Systems theory provides a holistic view of organisational processes, and organisational learning emphasizes the importance of continuous improvement. Finally, the resource-based view focuses on the strategic development of resources that provide competitive advantages. These theoretical foundations collectively contribute to the robustness and applicability of maturity models across different domains.
- (RQ4) Validation: The validation of maturity models involves a combination of qualitative and quantitative methods, including expert validation, questionnaires, focus groups, workshops, case studies, and survey-based validation. Statistical techniques such as factor analysis, Cronbach's alpha, structural equation modelling, and regression analysis are frequently employed to provide rigorous validation of the model's structure. The use of mixed methods, along with participatory approaches like workshops and action research, ensures that the model is both relevant to its intended users and grounded in empirical evidence.
- (RQ5) Domains: Maturity models have been applied across a wide range of domains, from e-government, Data Governance, Information Systems, Business Intelligence, IT Governance, Governance, Risk Management, Cloud Computing, Project Management and software development to cybersecurity and knowledge management, reflecting their versatility and adaptability. The concept of maturity models is applicable to both technical

and managerial disciplines, offering organisations a structured way to assess and improve their processes, capabilities, and systems.

5.3. Holistic Dark Data Governance Maturity Model

Maturity models are a strategic approach employed for the assessment and advancement of organisational capabilities (Saleh, M., 2011). The maturity model outlines a pathway for improving and advancing the organisational processes and capabilities (Frick, N., 2012). The maturity model typically encompasses a series of maturity levels, commonly ranging from one to five, where level one signifies a lack of maturity and level five denotes full maturity (Debreceeny, R. and Gray, L. G., 2013). The maturity model outlines a path that can help an organisation progress towards a mature state. According to Wibowo and Waluyo, maturity can be defined as the condition of being comprehensive, perfect, or ready for a specific purpose (Wibowo, A. M. and Waluyo, R., 2015). Maturity models enable organisations to assess their capabilities and competencies within a specific domain or problem context (Hamel, F. and Herz, T., 2013).

This research presents a maturity model that aims to define a path for enhancing the systemic functions of dark data governance within organisations. The dark data governance Maturity Model serves as a tool to assess an organisation's capacity to implement data governance for mitigating dark data risks. The model outlines key systemic functions to manage, measure, and control all aspects of dark data governance, drawing upon the holistic model for dark data governance developed in Chapter 4. Additionally, the model provides a mechanism for evaluating the current state of dark data governance awareness and effectiveness within the organisation.

This model enables organisations to assess their current dark data governance practices, identify gaps, and define new opportunities for implementation based on observable behaviours. Additionally, the model provides the following capabilities:

- Assess their current state of dark data governance and identify steps to improve it, in order to mitigate dark data risks and support their operational and strategic goals within the organisational context.
- Obtain an informed, objective, documented assessment of their dark data governance maturity.
- Gain knowledge of their existing dark data governance capabilities and understanding.

- Challenge internal assumptions and establish methods for consistently examining their dark data governance processes and practices.
- Define appropriate levels for improving dark data governance and develop a roadmap to govern more effectively across the organisation, in order to mitigate dark data risks and support their operational and strategic goals within the organisational context.
- Enable benchmarking and comparison: Maturity models enable organisations to benchmark their dark data governance practices against best-in-class standards or against peers within the same industry (Weber, K., Otto, B. and Osterle, H., 2009). By understanding the maturity level they have achieved, organisations can evaluate their strengths and weaknesses in relation to others and develop competitive advantages in managing dark data risks (DAMA., 2017).
- Encourage Organisational Learning: Maturity models emphasize the importance of continuous learning and improvement. By progressing through the levels, organisations can foster a culture of continuous assessment and adaptation. This approach allows them to respond effectively to new challenges in dark data governance (Fath-Allah, A. et al., 2014). It encourages organisations to learn from their mistakes, adjust their processes, and embed new governance practices across the organisation (DAMA., 2017).
- Provide Scalability and Sustainability: The maturity model provides a scalable framework that allows organisations to grow their governance practices over time. Whether they are small startups or large enterprises, the model's scalability ensures that governance improvements are sustainable and can be expanded as the organisation grows (Weber, K., Otto, B. and Osterle, H., 2009). At higher maturity levels, governance processes become embedded within the organisation's culture, ensuring long-term sustainability and alignment with business goals (DAMA., 2017).

The dark data governance maturity model is designed to enhance organisations' comprehension of their current state of dark data governance implementation and guide their future progress. This will be accomplished by categorizing the systemic functions of the holistic dark data governance model into five distinct maturity levels, ranging from an initial lack of maturity at level one to a state of full maturity at level five. This structured approach will enable organisations to assess their existing dark data governance capabilities and identify opportunities for improvement.

5.4. Dark Data Governance Maturity Model Development

As noted in the literature review in section 5.2, some of the existing maturity models in the literature were developed based on the concept construction of their area as the theoretical foundation. Therefore, the conceptual construction of dark data governance has been chosen as the theoretical foundation to develop the dark data governance maturity model in this chapter.

This study employs a three-phase approach to construct the proposed maturity model, comprising pre-design, design, and post-design phases. Each phase of maturity model development follows a structured process to achieve its objectives. Figure 5.1 outlines the approach used to develop the holistic dark data governance Maturity Model.

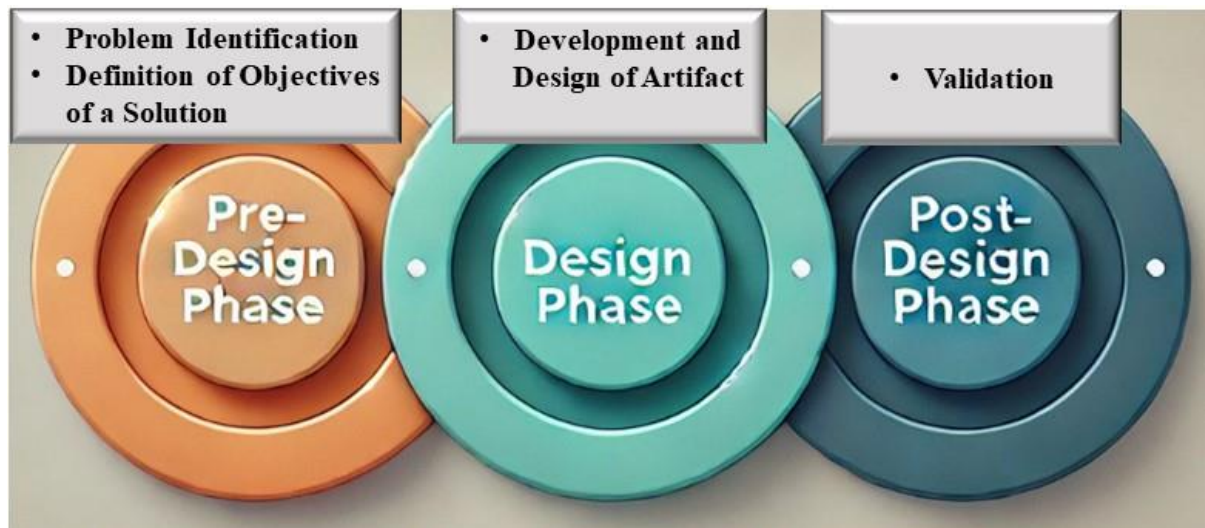


Figure 5. 1 Approach for constructing the dark data governance Maturity Model

The three-phase approach used to construct the proposed holistic dark data governance Maturity Model is described in Table 5.2.

Phase	Description
Pre-Design Phase	1.1 Problem Identification: This step involves understanding the issues or challenges that need to be addressed. Problem identification is a critical starting point, as the success of any design process depends on accurately identifying the core issue (Hevner, R, A. et al., 2004). This step ensures that the design process is grounded in real-world challenges.
	1.2 Definition of Objectives of a Solution After identifying the problem, the next step is to clearly define the objectives and goals that the solution should achieve. According to Peffers et al. (2007), defining objectives helps in

Phase	Description
	framing the desired outcomes and ensures that the solution aligns with the identified problem. These objectives serve as a guiding framework for the subsequent phases of the design (Peffer, K. et al., 2007).
Design Phase	2.1 Development and Design of Artifact: During this phase, the actual solution or artifact is designed and developed. Hevner et al. (2004) highlight that this step involves rigorous design and development based on theoretical knowledge and practical requirements. The artifact can be a model, method, or system, depending on the problem (Hevner, R. A. et al., 2004).
Post-Design Phase	3.1 Validation: Once the artifact has been developed, it undergoes a validation process to ensure it meets the defined objectives and requirements. Validation is critical in determining whether the designed solution functions as intended, providing feedback on its utility and relevance (Venable, J., Pries-Heje, J. and Baskerville, R., 2016).

Table 5. 2 Description of the three-phase Approach used to construct the dark data governance Maturity Model

5.4.1. Pre-Design Phase

The pre-design phase represents the foundational stage in developing the dark data governance Maturity Model. This phase serves to gain a comprehensive understanding of the research problem and objectives, encompassing two key steps: problem identification (Hevner, R. A. et al., 2004) and definition of objectives for a solution (Peffer, K. et al., 2007).

• Problem Identification

This step identifies the research problem and gaps through a literature review. The study systematically reviewed existing research on maturity models to understand the concept, the state of the problem, and available solutions. Based on the review results presented in Chapters 3 and 5, there appears to be a lack of research on maturity models and assessment matrices for dark data governance. The findings indicate that there are currently no established maturity models for dark data governance. According to Victor, organisations often lack awareness and understanding of their data governance mechanisms, with only a few individuals within the organisation being aware of the data governance processes in place (Victor, E., 2016). Consequently, maturity models for dark data governance are beneficial to gauge and evaluate the present state of dark data governance implementation within organisations.

• Definition of Objectives for a Solution

After identifying the problem, the next step is to clearly define the objectives and goals that the solution should achieve (Peffer, K. et al., 2007). This step defines the research goal and objectives of the dark data governance Maturity Model developed in this study to address the existing research gap. The proposed model serves as a solution aimed at assessing the maturity of holistic dark data governance within organisations. The maturity model design will be grounded in the holistic model presented in Chapter 4, which provides the theoretical foundation. The development of the maturity model will be further discussed in the subsequent section.

5.4.2. Design Phase

This phase focuses on the design and development of the proposed holistic dark data governance maturity model (Hevner, R. A. et al., 2004). According to the academic literature, the majority of existing maturity models were constructed using two key elements to accomplish their objectives: dimensions and maturity levels (Ryu, S. K., Park, S. J. and Park, J., 2006); (Saleh, M., 2011); (Fath-Allah, A. et al., 2014). This study constructed the proposed holistic dark data governance Maturity Model using three principal elements:

- Improvement Mechanisms (Wiener, N., 1948), (Beer, S., 1959)
- Maturity Model Dimensions (holistic dark data governance systemic functions), and
- Defined maturity levels.

This section aims to outline the proposed holistic dark data governance maturity model and its underlying dimensions and sub-dimensions. The development of the maturity model involves three key steps. First, it is necessary to identify the improvement mechanisms that will be integrated into the model. Second, the maturity model dimensions, and sub-dimensions will be constructed upon the holistic model's systemic functions, as presented in Chapter 4. Finally, the maturity levels used to assess the systemic functions must be defined and named in alignment with the holistic dark data governance context. Figure 5.2 depicts the architectural approach of the proposed holistic dark data governance maturity model, and the subsequent sections provide a detailed explanation of the model's dimensions and sub-dimensions.

5.4.2.1. Improvement Mechanisms

This component represents the anticipated improvement mechanisms that will be enabled by implementing the dark data governance maturity model within the organisational VSM context.

Existing literature on maturity models indicates common improvement mechanisms employed.

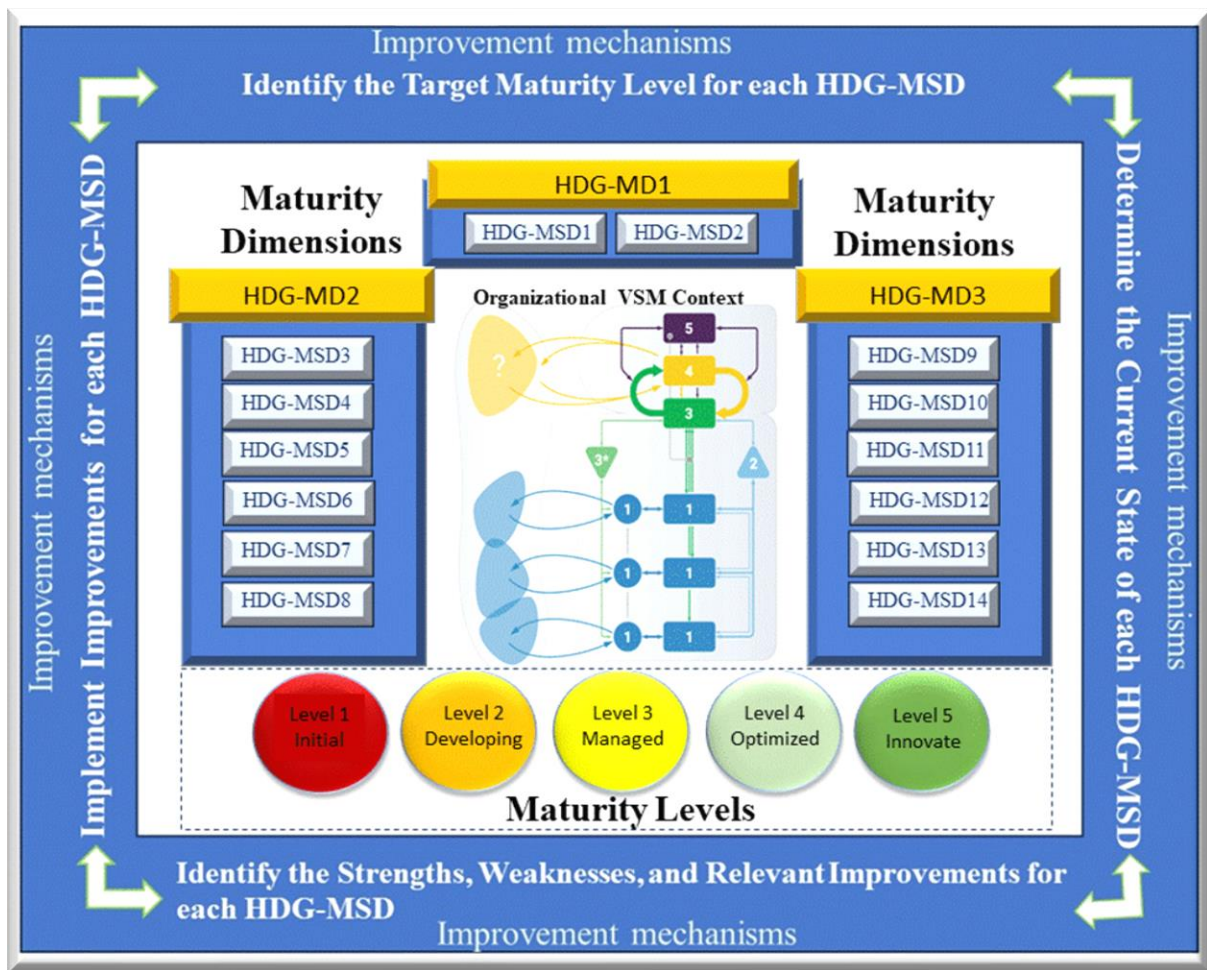


Figure 5. 2 Holistic Dark Data Governance Maturity Model Architecture within the Organisational VSM Context

Accordingly, the dark data governance maturity model developed in this research is intended to facilitate critical enhancements that will help organisations achieve appropriate maturity levels for their dark data governance deployments. Improvement mechanisms are critical in maturity models, as they ensure that organisations can continuously assess and refine their processes. **Feedback loops** allow for real-time evaluation of the maturity model and are essential for fostering continuous improvement (Argyris, C. and Schön, A. D., 1978). Feedback can be collected through various channels, such as **internal assessments**, **external audits**, and **self-evaluation tools**. In the context of holistic dark data governance, improvement feedback mechanisms often involve regular reviews of dark data, compliance, and governance practices. These feedback loops ensure that the maturity model remains adaptable to changes in technology, regulations, and organisational objectives. De Bruin et al. (2005) suggest that

maturity models should include feedback mechanisms at every level of maturity to ensure the model's practical relevance and sustainability (De-Bruin, T. et al., 2005). The following steps are necessary for the improvement feedback mechanism:

The expected steps of the improvement mechanism within the VSM Organisational Context are outlined in Figure 5.3 and described below:

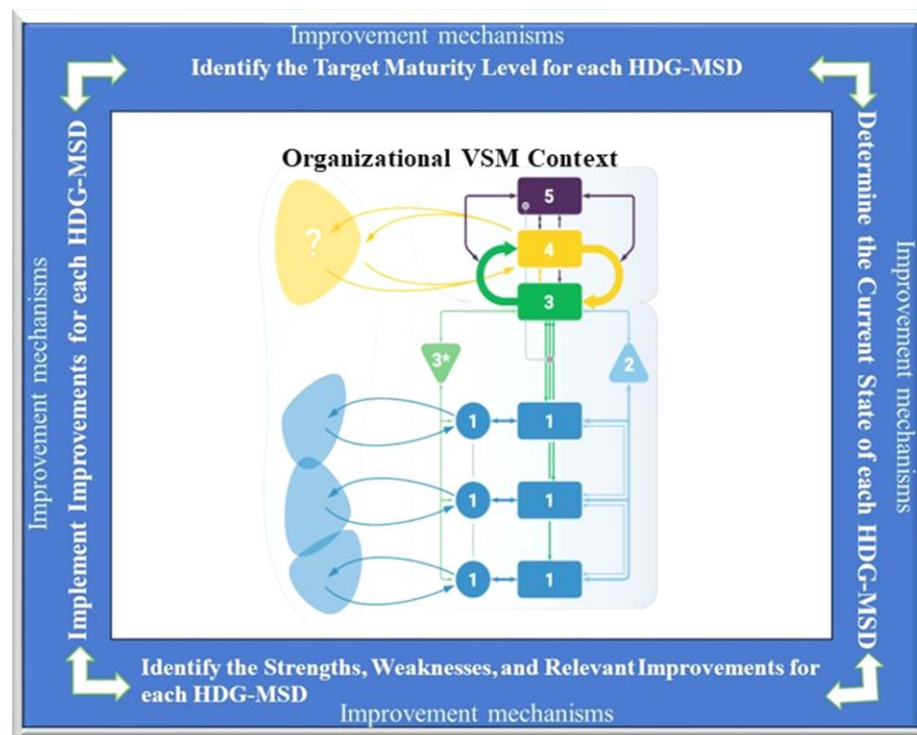


Figure 5. 3 Holistic Dark Data Governance Maturity Model Improvement Mechanisms within the Organisational VSM Context

a) Identify the Organisation's Target Maturity Level for Dark Data Governance Systemic Functions

The holistic dark data governance Maturity Model will outline the overall maturity levels as well as the maturity level for each systemic function of dark data governance. Informed by the organisation's data governance requirements to support its business objectives and the current state of its dark data governance, the target maturity level for dark data governance will be selected. Once the maturity levels of the systemic functions have been defined and evaluated, the next step is to determine the organisation's target maturity level for each systemic function (Saleh, M., 2011), (Rivera, E. et al., 2017). Accordingly, the systemic functions of dark data governance should function at a target maturity level to effectively manage dark data and

support the achievement of the organisation's operational and strategic objectives within the organisational Viable System Model context (Beer, S., 1981), (Beer, S., 1979).

b) Determine the Current State of Dark Data Governance Systemic Functions

Implementing the holistic model enables organisations to determine and assess the current state of their dark data governance. This component's expected outcome is to assist organisations in improving their dark data governance systemic functions. This will enhance the mitigation of dark data and support the achievement of organisational goals within the organisational Viable System Model context (Beer, S., 1981).

c) Identify the Strengths, Weaknesses and Relevant Improvements of Dark Data Governance Systemic Functions

One of the key outcomes of the holistic dark data governance maturity model is that it enables organisations to identify the strengths and weaknesses of their existing dark data governance implementation. These strengths and weaknesses pertain to the positive and negative factors that are directly under the control of the organisation or its decision-makers. Thus, to achieve an effective implementation of dark data governance, the organisation must thoroughly evaluate and determine the relevant strength, weakness, opportunity, and threat factors that influence its data governance capabilities (Rivera, E. et al., 2017). After evaluating the current state of its dark data governance, the organisation can identify the positive and negative factors, as well as opportunities for improvement and potential threats, that influence its data governance capabilities.

d) Improve Dark Data Governance Systemic Functions

Implementing the identified improvements to the dark data governance systemic functions is essential for enhancing the capability of the holistic dark data governance approach to support the achievement of the organisation's operational and strategic objectives. This allows the organisation to better manage the complexity and dynamically adapt its data governance mechanisms to evolving data environments, thereby improving efficiency and minimizing risks associated with dark data. Improving dark data governance within the Viable System Model (VSM) context is crucial for enhancing organisational data governance maturity. Dark data, often unmanaged and unutilized, poses risks such as non-compliance, inefficiencies, and missed opportunities for insight (Hand, J. D., 2020), (Saleh, M., 2011). The holistic data governance approach aligns governance functions with organisational processes, ensuring visibility, risk mitigation, and efficient resource use (Beer, S., 1984), (Espejo, R. and Reyes,

A., 2011). Therefore, when organisations implement the dark data governance maturity model, it will help them to improve their dark data governance systemic functions by understanding their position and enhancing their ability to manage complexity and dynamically adapt governance mechanisms to evolving data environments (Ashby, R, W., 1956), (Leonard, A., 2009). As such deploying dark data governance maturity approach is essential for developing effective dark data governance strategies and achieving higher maturity levels (Fath-Allah, A. et al., 2014), (Ryu, S, K., Park, S, J. and Park, J., 2006). Improving holistic dark data governance allows organisations to manage complexity, improve efficiency, and minimize risks. This is essential for achieving higher maturity levels in holistic dark data governance, enabling organisations to turn dark data into valuable assets.

5.4.2.2. Holistic Dark Data Governance Maturity Dimensions

The maturity model dimensions refer to the crucial domains or components that are used by the maturity model to comprehensively measure and evaluate the different aspects of the field of study. These dimensions provide a structured framework for assessing the maturity and capabilities of the system or process under evaluation (Adler, S., 2007). In developing a maturity model, it is important to first define the key components or attributes that will be assessed in order to fulfil the model's intended purpose (Rose, J. and Guide, P., 2013). According to Laszlo and Krippner (1998), systems theory provides a holistic view of organisations, suggesting that different components, including processes, technologies, and people, must work together harmoniously within a systemic context for continuous improvement (Laszlo, A. and Krippner, S., 1998). Accordingly, the systemic functions of the proposed holistic model presented in Chapter 4 were chosen as the dimensions for the maturity model in this research. The decision to use these systemic functions as the HDG Maturity Dimensions was intentional, as it aligns with the holistic systems theory approach. This ensures that the maturity model comprehensively covers all the critical components required for effective holistic dark data governance. The systemic functions of holistic dark data governance within the organisational Viable System Model context, as depicted in Figure 5.4 and detailed in Table 5.3, constitute the holistic data governance maturity dimensions (HDG-MDs) and sub-dimensions (HDG-MSDs) for the maturity model proposed in this research.

Building the maturity model around the key systemic functions of holistic dark data governance within the organisational Viable System Model context ensures a comprehensive model that covers all critical aspects of data governance (Ladley, J., 2012). This structured, systems-based

approach enables organisations to progressively enhance their data governance capabilities and ensure alignment with broader business goals and objectives. The dimensions and sub-dimensions of the proposed HDG maturity model, as discussed in detail in Chapter 4, provide a robust framework for measuring and assessing the maturity of holistic dark data governance in organisations. Each dimension of the HDG maturity model, such as the organisational VSM context, systemic functions, and their interactions, will be evaluated based on its corresponding sub-dimensions and associated maturity levels. The specific HDG maturity sub-dimensions (HDG-MSDs) that will be used to comprehensively assess the organisation's data governance capabilities are illustrated in Table 5.3 for each HDG maturity dimension (HDG-MD).

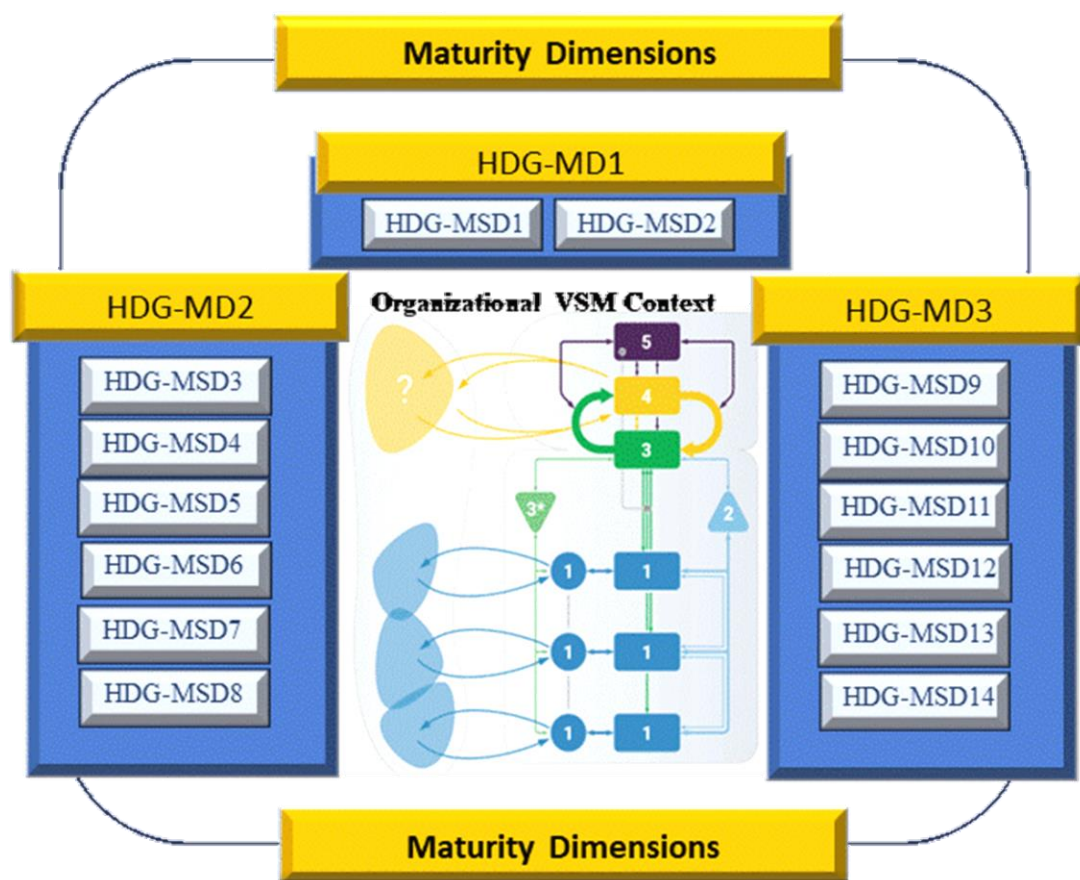


Figure 5. 4 The Holistic Dark Data HDG Maturity Dimensions and Sub-Dimensions

Dimension (HDG-MD)	Assessed by (Sub-Dimensions: HDG-MSDs)
HDG-MD1: Organisational VSM Context and Dark Data	HDG-MSD1: VSM Organisational Context and Goals: The process begins by defining the organisation's context (business scope, business operational and strategic goals) and aligning the specific goals for dark data governance goals with organisational broader goals and objectives.

Dimension (HDG-MD)	Assessed by (Sub-Dimensions: HDG-MSDs)
Governance Scope and Goals	HDG-MSD2: Recursive Organisational Levels and HDG Scope: While recursive levels can be considered, this study focuses on the organisational level with a clearly defined manageable scope of holistic dark data governance. The model can be applied at any other level of organisational recursion, as it maintains the same structural context. This study identified an organisational level as the system-in-focus. Accordingly, defined the scope for dark data governance within the holistic organisational context to support the achievement of goals.
HDG-MD2: Holistic Dark Data Governance (HDG) Systemic Functions (SFs) within the Organisational VSM Context	HDG-MSD3: Systemic Functions (SF1): This represents the HDG systemic functions to ensure the deployment of data governance systemic functions within the organisational VSM operational units (S1) to support their delivery of the organisational core products and services.
	HDG-MSD4: Coordination (SF2): This function prevents conflicts within the organisation and ensures alignment with corporate policies.
	HDG-MSD5: Control (SF3): This function ensures cohesion and autonomy of HDG systemic functions across the organisation. It includes corporate policies regarding data architecture, data quality, metadata, security, and more, and the allocation of HDG resources to SF1.
	HDG-MSD6: Auditing and Compliance (SF3*): Auditing functions gather and evaluate data governance-related information to maintain regulatory and policy compliance.
	HDG-MSD7: Adaptation (SF4): This function assesses external environmental changes and shapes long-term data governance strategies to maintain organisational agility.
	HDG-MSD8: Policy, Identity, and Closure Functions (SF5): This function supports consistent corporate dark data governance identity and ensures cohesive and integrated governance of relevant domains across all organisational levels.
HDG-MD3: Interactions of Holistic Dark Data Governance (HDG) Systemic Functions within the Organisational VSM Context	HDG-MSD9: Recursivity Levels Integration (SF6): This systemic function ensures integration with other relevant data governance systemic functions at different recursion levels. It also ensures integration across different governance within the same level. This is essential to counteract dark data and support the achievement of operational and organisational embedded goals.
	HDG-MSD10: Requisite Variety Systemic Function (SF7): This systemic function addresses the variety needed to govern data assets and dark data risks, supporting operational and strategic organisational goals amidst external disruptions.

Dimension (HDG-MD)	Assessed by (Sub-Dimensions: HDG-MSDs)
	HDG-MSD11: Effective Inter-Operational Management (SF8): Ensures that data governance systemic functions within the organisational VSM operational units interact with coordination and control functions to support organisational goals.
	HDG-MSD12: Metasystem Adaptability, Learning, and Change Management Systemic Functions (SF9): Represents interactions among SF3, SF4, and SF5 (Metasystem), providing holistic decision-making, adaptability, and change management in data governance and dark data handling activities.
	HDG-MSD13: Communication Channels and Algedonic Channel Systemic Functions (SF10): Represents communication channels and their interactions across all systems to mitigate dark data risks. Algedonic channels trigger immediate responses in crises or high-risk situations.
	HDG-MSD14: Transduction and Integration of All Systems - Common Data Governance Knowledge Systemic Functions (SF11): Ensures interactions among all systems to integrate operations, reduce silos, and promote organisational stability, supporting the achievement of organisational goals.

Table 5. 3 HDG -Dimensions and their respective sub-dimensions

5.4.2.3. Holistic Dark Data Governance Maturity Levels

The proposed holistic dark data governance Maturity Model presents a comprehensive scale for assessing and evaluating the maturity of an organisation's dark data governance practices and the capability of its dark data governance systemic framework within the organisational VSM context. Assessing the maturity of dark data governance can be a significant challenge for stakeholders and decision-makers, as it requires determining the level of governance achieved through data governance investments (Owuonda, S. and Orwa, D., 2016). Additionally, estimating the future effectiveness of these investments in protecting data is difficult, as data protection policies, regulations, and the threat environment are constantly evolving (Saleh, M., 2011). To address these challenges, organisations can develop a dark data governance Maturity Model that allows them to evaluate their systemic functions against a clear set of best practice benchmarks (Caralli, A, R., Knight, M. and Montgomery, H, A., 2012). These benchmarks typically represent industry standards or codes of practice that are important for the specific domain or discipline. The proposed holistic dark data governance Maturity Model consists of five distinct levels, each representing a different stage of

organisational maturity in holistic dark data governance within the organisational VSM context: Level 1: Initial dark data governance, Level 2: Developing dark data governance, Level 3: Managed dark data governance, Level 4: Optimized dark data governance, and Level 5: Innovative dark data governance.

The distinct levels in this maturity model represent sets of objectives that, when met, strengthen a crucial element of the holistic dark data governance framework. Attaining each level of the dark data governance Maturity Model establishes a different component in the implementation of dark data governance, leading to a progressive enhancement in the organisation's capability to achieve effective holistic dark data governance. As the organisation advances to higher levels, its holistic dark data governance is expected to improve. Furthermore, Section 5.5.1 below will present the formulation of cell text to determine the characteristics of these levels, in order to assess the maturity of the dark data governance implementation based on the systemic functions of the HDG Model in this research. The holistic dark data governance maturity levels are as depicted in Figure 5.5 and described in Table 5.4.

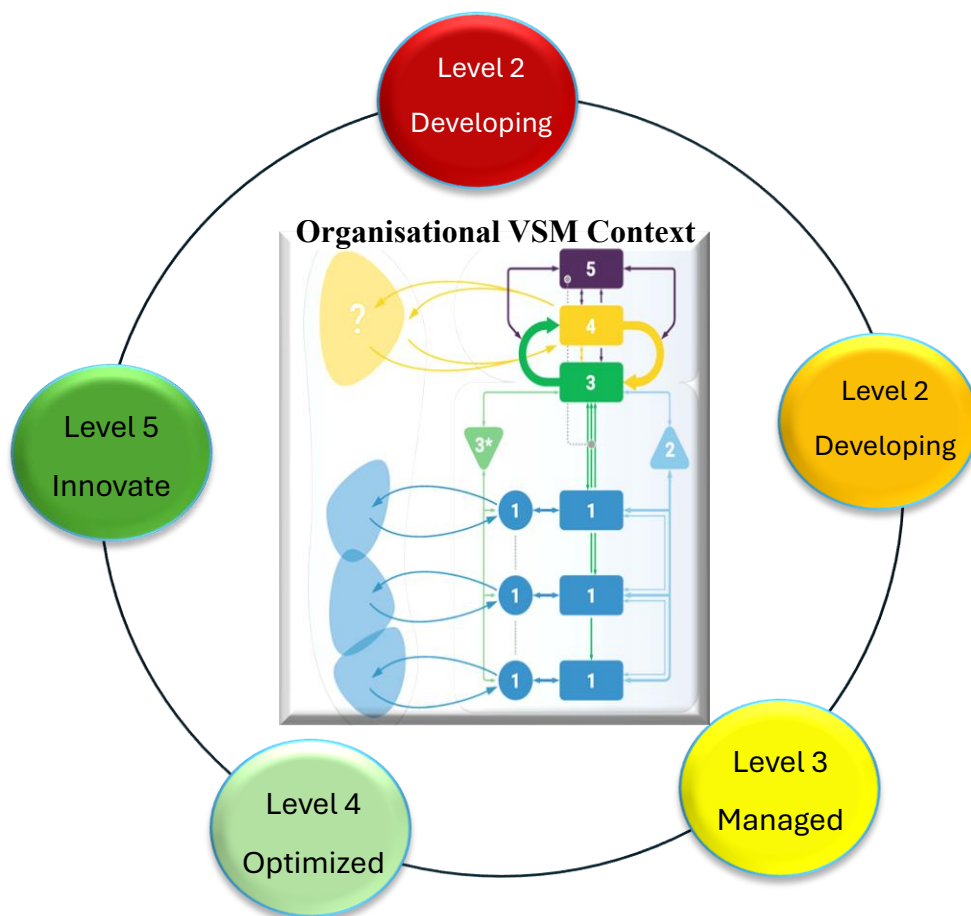


Figure 5. 5 The dark data governance maturity levels within the organisational VSM context

Maturity Level Name	Description
Level 1: Initial (Ad-hoc)	Data governance practices are informal, inconsistent, and reactive. There are no formal policies, and issues are addressed on an as-needed basis (Ladley, 2012). Organisations at this stage often lack formal data governance structures and rely on individual efforts without cohesive oversight.
Level 2: Developing (Defined)	Basic data governance policies are defined, but implementation is inconsistent. Data management responsibilities are assigned, but there may be gaps in enforcement (Becker et al., 2009). At this level, organisations start to formalize governance processes but often face challenges in maintaining consistency across departments.
Level 3: Managed (Proactive)	Data governance processes are well-defined and consistently applied. Governance policies are integrated into everyday business practices, with a focus on data quality and compliance (DAMA, 2017). Organisations are proactive in managing data governance, using performance metrics to measure data quality, accessibility, and compliance.
Level 4: Optimized (Predictive)	Data governance is fully integrated into the organisation's culture and processes. Advanced practices, like predictive analytics for data quality management and continuous improvement, are in place (Ladley, 2012). Organisations use advanced analytics and automation to monitor and enhance governance practices continually.
Level 5: Innovative (Adaptive)	Data governance is fully adaptive, allowing rapid responses to new data challenges and regulatory changes. Organisations continuously innovate and improve their governance frameworks (Becker et al., 2009). Data governance is deeply embedded into the culture and operationalized across all functions (Saleh, 2011).

Table 5. 4 Maturity levels and their descriptions

5.4.3. Post-Design Phase

This post-design phase aims to validate the proposed holistic dark data governance maturity model to ensure that it achieves its intended objectives. The literature review findings presented in this chapter (Section 5.2.) indicated that the most common validation methods used in prior research include expert validation, questionnaires, focus groups, workshops, case studies, and survey-based validation. Therefore, this study has chosen to conduct an expert validation using the Delphi technique within a university in Texas, USA (University X) to validate the maturity model. The results of this validation process will be considered and used to improve the

maturity model, ultimately ensuring its effectiveness. The detailed validation process and its results will be presented in Chapter Seven.

5.5. Assessment Matrix

The enhancement and advancement of organisational capabilities represents a complex challenge (Maier, A., Moultrie, J. and Clarkson, J, P., 2012). Organisational performance assessments are frequently utilized to support management decision-making and facilitate continuous improvement. One method of evaluating an organisation's capabilities is through the use of an assessment matrix. While assessment matrices may share a similar underlying structure, their specific content often varies and is typically developed customized to the organisation's needs (Maier, A., Moultrie, J. and Clarkson, J, P., 2012), (Blommerde, T. and Lynch, P., 2016). An assessment matrix is a tool used to evaluate the level of development or maturity of a specific process or program within an organisation. It serves as a systematic checklist to assess how well-established and implemented a particular operational or management framework is (Barnes, E. et al., 2012). Another definition of a maturity or assessment matrix describes it as a management tool used to evaluate an organisation's level of progress towards a specific objective or goal (Galán, A. et al., 2017). There is a wealth of assessment matrices in the literature that have been developed by researchers and practitioners to assess organisations across a diverse range of fields and industries (Pohlman, M., 2010), (Barnes, E. et al., 2012), (Maier, A., Moultrie, J. and Clarkson, J, P., 2012), (Blommerde, T. and Lynch, P., 2016). The majority of these assessment matrices have been designed based on specific process areas and maturity levels associated with particular domains. In the case of data governance assessment matrices, they are typically developed as interactive diagnostic tools to evaluate both the current state of an organisation's data governance preparedness and its corresponding maturity level (Adler, S., 2007), (Rivera, E. et al., 2017). Existing research indicates that various scholars and industry entities, such as IBM, SAS, and Stanford University, have designed assessment frameworks to evaluate data governance practices within organisations (Adler, S., 2007), (Nascio., 2009). These assessment matrices have been developed to assess data governance in general based on their framework dimensions. Maier et al. (2012) proposed a four-phase roadmap with key decision points and steps for developing an assessment matrix, which includes: planning, development, evaluation, and maintenance phases.

- The planning phase involves specifying the target audience, defining the aim, clarifying the scope, and establishing success criteria.

- The development phase encompasses selecting the process areas (content), determining the maturity levels (rating scale), formulating the cell text (intersection of process areas and maturity levels), and defining the administration mechanism.
- The evaluation phase focuses on validation and verification.
- The maintenance phase includes checking benchmarks, maintaining a results database, and documenting and communicating the development process and results.

Figure 5.6 shows the phases and decision points of the roadmap to develop an assessment matrix.

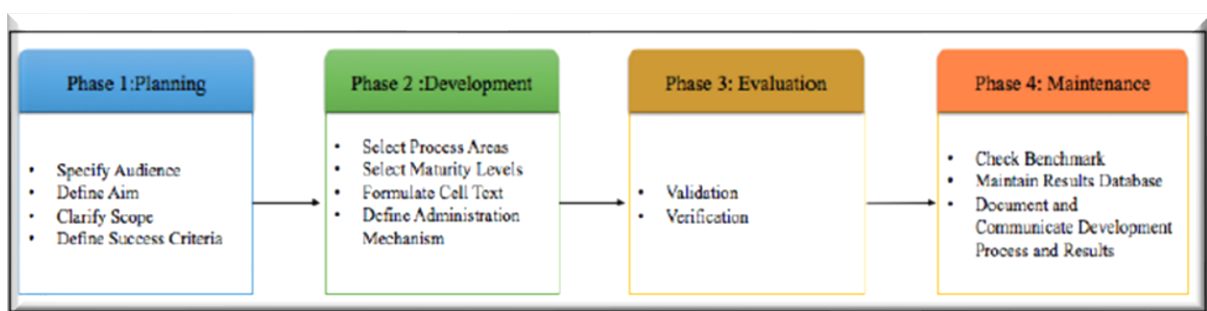


Figure 5. 6 Phases and decision points of the roadmap to develop an assessment matrix.
Source: (Maier et al., 2012)

The holistic dark data governance assessment matrix developed in this study is an application of the maturity model for the domain of dark data governance. The assessment matrix serves as a tool to evaluate the current state of holistic dark data governance within an organisation. It helps the organisation identify its target state for effective dark data governance that support the achievement of the organisational goals. Furthermore, the dark data governance assessment matrix aims to pinpoint the strengths and weaknesses of the organisation's holistic dark data governance practices and provides guidance to enhance dark data governance across the organisation to support the achievement of the organisational goals. The literature indicates that maturity models and assessment matrices are distinct concepts. Maturity models focus on defining the scope of assessment based on process areas and maturity levels, whereas assessment matrices take a more detailed approach to evaluating an organisation's state of maturity (Schipper, J., 2002), (Maier, A., Moultrie, J. and Clarkson, J, P., 2012). The next section will present and discuss the development of the assessment matrix for holistic dark data governance.

5.5.1. Development of the Holistic Dark Data Governance Assessment Matrix

This study developed a holistic dark data governance assessment matrix to support the holistic dark data governance maturity model presented in this thesis. The proposed maturity model was designed to define an organisation's maturity level based on the holistic dark data governance model developed in Chapter 4. The dark data governance maturity model utilizes two core components to analyse the state and enhance the processes of dark data governance within the organisation: dark data governance dimensions and maturity level. This study has adopted the development and evaluation phases proposed by Maier et al. (2012). This chapter discusses the development process of the holistic dark data governance assessment matrix, while the validation of the matrix will be presented in Chapter Seven.

The dark data governance assessment matrix was developed based on three key components: the dark data governance dimensions, the maturity levels, and the formulated cell text descriptions (intersection of dimensions and maturity levels). As discussed in the preceding section on the maturity model, the dark data governance dimensions and maturity levels have already been established. The selection of relevant process areas and appropriate maturity levels is instrumental in formulating the cell text descriptions, which in turn serve as the foundation for the assessment matrix (Maier, A., Moultrie, J. and Clarkson, J, P., 2012), (Moultrie, J., Sutcliffe, L. and Maier, A., 2016). Formulating the cell text descriptions is a crucial step in developing an assessment matrix. The literature suggests that once the relevant process areas and maturity levels for each dimension have been identified, one of the most important tasks is to define the behavioural characteristics associated with those processes at each level of maturity (Barnes, E. et al., 2012), (Maier, A., Moultrie, J. and Clarkson, J, P., 2012), (Blommerde, T. and Lynch, P., 2016), (Moultrie, J., Sutcliffe, L. and Maier, A., 2016). Moreover, the process characteristics must be described for each maturity level, with each successive level building upon the previous ones. For instance, to attain level 3 maturity, the requirements of levels 1 and 2 must also have been fulfilled. Consequently, the descriptions should be straightforward, clear, and concise (Maier, A., Moultrie, J. and Clarkson, J, P., 2012), (Rose, J. and Guide, P., 2013).

Distinguishing between maturity levels in an assessment matrix necessitates several critical considerations (Maier, A., Moultrie, J. and Clarkson, J, P., 2012), (Moultrie, J., Sutcliffe, L. and Maier, A., 2016):

- determining whether the cell text descriptions should be prescriptive or descriptive in nature

- justifying the source of information used to formulate the text
- deciding on the appropriate mechanism to develop the text descriptions

In this study, these decision points were taken into account to differentiate between the maturity levels in the holistic dark data governance assessment matrix. The cell text descriptions were formulated using a descriptive approach, which entails providing a detailed account of the individual case and considering various aspects, such as the underlying rationale, characteristics, and domain knowledge (Maier, A., Moultrie, J. and Clarkson, J, P., 2012).

As for the source of information, the literature provides various options to formulate the text descriptions for each cell of the assessment matrix (Maier, A., Moultrie, J. and Clarkson, J, P., 2012), (Moultrie, J., Sutcliffe, L. and Maier, A., 2016). One approach to formulating the assessment matrix cell text descriptions is to synthesize viewpoints from a sample of individuals representative of the intended assessment recipients. Alternatively, the cell text can be developed by reviewing and comparing the practices of multiple organisations, such as through empirical studies, analysis of written case studies in the literature, and examination of best practice guides. This study relies on reviewing best practice guides from the literature to inform the formulation of the assessment matrix. These findings will then be validated and evaluated by experts from a leading university in Texas, USA by deploying the Delphi method. Regarding the mechanism for developing the text descriptions, the literature indicates that identifying the extreme ends of the maturity scale is a common approach (Barnes, E. et al., 2012) (Moultrie, J., Sutcliffe, L. and Maier, A., 2016) (Maier, A., Moultrie, J. and Clarkson, J, P., 2012) (Blommerde, T. and Lynch, P., 2016). Accordingly, this study adopts this mechanism to determine the best and worst practices, and then characterize the intermediate maturity levels in between. When formulating the text descriptions for each level of the assessment matrix, it is crucial to create clear distinctions between the levels to enable an accurate diagnosis of the organisation's maturity state and avoid confusion. The assessment matrix utilizes a set of differentiated maturity levels to characterize the degree to which each sub-dimension or component of the holistic dark data governance model has been formally adopted and integrated into the organisation's structure. These maturity levels range from Ad-hoc, where the adoption is reactive and informal and reactive, to Defined, Proactive, Predictive, and ultimately Adaptive, where the sub-dimensions are fully embedded into the organisation's processes and systems in a proactive and adaptable manner.

Table 5.5 shows the critical considerations to differentiate between the maturity levels in the assessment matrix.

Decision Point	Description
Determining whether the cell text is prescriptive or descriptive	Descriptive Approach
Information Source	Reviewing written case studies in literature, and best practice guides from excellence initiatives
Mechanism of formulating the text descriptions	Determine the best and worst practices, and then, determine the characteristics of all the levels in between

Table 5. 5 Critical considerations to distinguish between the maturity levels in the maturity matrix

The proposed assessment matrix was constructed with five distinct maturity levels, and three core reference categories were incorporated to enable cross-comparison across the maturity levels. The resulting assessment matrix contained detailed descriptions of the organisational processes and their performance at each level of maturity, with each successive level building upon the previous one. The sub-dimensions for each component of the holistic dark data governance model were embedded within this assessment matrix. The assessment matrix for each dimension is outlined as follows:

- **HDG-MD1 Assessment Matrix: Organisational VSM Holistic Context and Dark Data Governance Scope and Goals**

This assessment matrix aims to characterize the maturity level of the organisation by evaluating its Organisational VSM Holistic Context and Dark Data Governance Scope and Goals. This HDG maturity dimension (HDG-MD1) is assessed through two maturity sub-dimensions (HDG-MSDs): HDG-MSD1 and HDG-MSD2.

- **HDG-MSD1: VSM Organisational Context and Goals:** examines the VSM Organisational Holistic Context and Goals and Dark Data Governance Goals, which involves defining the organisation's business operational and strategic context and aligning the specific goals for dark data governance with its broader strategic objectives.
- **HDG-MSD2: Recursive Organisational Levels and HDG Scope:** assesses the identification of the holistic dark data governance scope at the selected recursive Level within the multiple VSM Organisational recursive levels to support organizational goals.

Table 5.6 presents the maturity levels for the two sub-dimensions of the HSG-MD1, offering organisations a structured framework to evaluate their current state and pinpoint areas for improvement in dark data governance within the organisational holistic context. This approach aims to mitigate dark data challenges and support the achievement of the organisation's operational and strategic objectives.

Sub-Dimensions / Levels	Level 1: Initial (Ad-hoc)	Level 2: Developing (Defined)	Level 3: Managed (Proactive)	Level 4: Optimized (Predictive)	Level 5: Innovative (Adaptive)
HDG-MSD1: VSM Organisational Context and Goals	Holistic dark data governance goals are unclear and not aligned with the organisation's business context or strategic business objectives. The process is informal and reactive, with little consideration for long-term planning within an organisational systemic context	Basic dark data governance goals are defined, but alignment with broader organisational business goals is inconsistent. Initial attempts to connect governance practices to strategic objectives within an organisational systemic context	Dark data governance goals are consistently aligned with organisational business context and strategic objectives. Integrated into business practices, focusing on compliance and dark data. Proactive systemic context.	Holistic dark data governance is fully integrated into the organisation's business systemic context. Goals are continuously refined, using predictive analytics and proactive planning to respond to changing strategic objectives within a business systemic context	Holistic dark data governance is highly adaptive, allowing rapid response to new dark data challenges. Governance is embedded into corporate business strategic planning, continuously evolving to meet changing objectives within the organisational business systemic context
HDG-MSD2: Identifying Recursive Organisational Level and HDG Scope	No identification of HDG scope and business recursive organisational level. Efforts are isolated at the top level	Some recognition of the HDG scope and the recursive business level, but the application of dark data governance	HDG scope and recursive organisational level are identified and incorporated into a systemic context. There is a	Advanced methodologies monitor and adjust dark data governance scope at the identified organisational level.	HDG scope is fully adaptive and defined organisation wide. Real-time adjustments support evolving HDG scope

Sub-Dimensions / Levels	Level 1: Initial (Ad-hoc)	Level 2: Developing (Defined)	Level 3: Managed (Proactive)	Level 4: Optimized (Predictive)	Level 5: Innovative (Adaptive)
	without a structured systemic approach for considering HDG scope at the organisational holistic context.	scope is limited, and gaps exist in extending governance to the organisational holistic context.	structured approach to enhancing dark data governance scope across levels to align with business needs.	Adaptive mechanisms address HDG scope changes across various organisational systemic levels.	to support achievement of the operational and strategic goals within a systemic context

Table 5. 6 HDG-MD1 Assessment Matrix

- **HDG-MD2 Assessment Matrix: Holistic Dark Data Governance (HDG) Systemic Functions (SFs) within the Organisational VSM Context**

This assessment matrix aims to characterize the maturity level of the organisation by evaluating its holistic Dark Data Governance (HDG) systemic Functions (SFs) within the Organisational VSM Context. This HDG maturity dimension (HDG-MD2) is assessed through the following six maturity sub-dimensions (HDG-MSDs):

- **HDG-MSD3:** Deployment context Systemic Functions (SF1): Deployment of HDG Systemic Functions: This represents the deployment of HDG systemic functions for dark data management within the organisation's operational business units, integrated with other governance domains. This supports the achievement of the organisation's operational and strategic goals.
- **HDG-MSD4:** Coordination Systemic Functions (SF2): This function prevents conflicts within the organisational deployment of holistic dark data management and ensures compliance with HDG policies, procedures, and guidelines in alignment with corporate policies. This supports the achievement of the organisation's operational and strategic goals.
- **HDG-MSD5:** The Control Systemic Functions integrate with other governance domains to support a balanced approach between self-regulation for individual business operational units and their synergistic alignment for enhanced organisational performance and the achievement of operational and strategic objectives. This includes management of data governance compliance, performance, legal and regulatory

adherence, resource allocation, accountability assignment, and policy development across data governance domains.

- **HDG-MSD6:** Auditing and Compliance (SF3*): The Auditing and Compliance function enables the Control Systemic Functions to gather information about dark data challenges and governance operations from business operational units. This function focuses on auditing and compliance evaluations to ensure accuracy and adherence to data governance policies and standards, with the results shared to inform corrective actions. The purpose of this function is to support the achievement of the organisation's operational and strategic objectives.
- **HDG-MSD7:** Adaptation (SF4): This function assesses external environmental changes, such as constraints and opportunities related to data needed by organisations, as well as the potential impact of dark data on organisational viability. It then formulates long-term data governance strategies and related activities, such as market analysis and corporate planning, to maintain organisational adaptability and support the achievement of the organisation's long-term goals.
- **HDG-MSD8:** This function represents the highest level of decision-making within the selected organisational level of recursion, thereby providing logical closure to the holistic dark data governance subsystem (SF5). It supports the establishment of a consistent corporate identity to enable the deployment of coherent dark data governance systemic functions across business operations within a holistic context. Furthermore, this function sets the overall strategic direction, policies, values, and purpose of the holistic dark data governance system, and monitors the feedback loop between the current and future state of the data governance functions. This ensures a balance between internal and external perspectives, thereby supporting the achievement of both short-term operational and long-term organisational goals.

Table 5.7 outlines the maturity levels for the six maturity sub-dimensions of HDG-MD2, offering organisations a structured framework to evaluate their current state and pinpoint areas for improvement in dark data governance within the organisational holistic context. This approach aims to mitigate dark data challenges and support the achievement of the organisation's operational and strategic objectives.

Sub-Dimensions / Levels	Level 1: Initial (Ad-hoc)	Level 2: Developing (Defined)	Level 3: Managed (Proactive)	Level 4: Optimized (Predictive)	Level 5: Innovative (Adaptive)
HDG-MSD3: Deployment Context Systemic Functions (SF1)	Dark data governance informal deployment of HDG systemic functions. Dark data management is isolated, unstructured, and not aligned with other governance domains.	Basic HDG functions are defined but implemented inconsistently across business units. Limited integration with other governance domains.	HDG systemic functions are well-defined and integrated into operational business units. Aligned with other governance domains to support organisational goals.	HDG is fully integrated with business units. Advanced tools and predictive analytics are used for efficient deployment of HDG systemic functions, aligned with strategic objectives.	HDG functions are fully adaptive and deployed organisation wide. Real-time adjustments support evolving operational and strategic goals, enhancing performance.
HDG-MSD4: Coordination Systemic Functions (SF2)	Dark data governance coordination is reactive, and conflicts are addressed on an as-needed basis. Compliance with HDG policies is minimal and inconsistent.	Dark data governance basic coordination functions exist, but there are gaps in policy enforcement. Some alignment with corporate policies, but not across all units.	Dark data governance has well-defined coordination mechanisms in place to ensure compliance with HDG policies and prevent conflicts. Aligned with corporate policies consistently.	Dark data governance has advanced coordination mechanisms and uses predictive analytics to proactively prevent conflicts. Full compliance with HDG policies across all business units.	Dark data governance adaptive coordination that evolves with organisational changes. HDG Policies are updated dynamically to align with corporate strategies and external factors.
HDG-MSD5: Control Systemic Functions (SF3)	Dark data governance control functions are minimal, with limited oversight of dark data governance practices. No integration with other	Dark data governance basic control mechanisms exist but lack consistency. Initial efforts to integrate with other governance domains are fragmented and siloed.	Dark data governance control functions are structured and integrated with other governance domains. A balanced approach supports self-regulation and	Dark data governance advanced control mechanisms use automation and analytics to monitor compliance, resource allocation, and policy	Dark data governance has fully adaptive control functions that evolve based on feedback and organisational needs. HDG Supports strategic

Sub-Dimensions / Levels	Level 1: Initial (Ad-hoc)	Level 2: Developing (Defined)	Level 3: Managed (Proactive)	Level 4: Optimized (Predictive)	Level 5: Innovative (Adaptive)
	governance domains.		alignment for performance.	adherence dynamically.	direction and long-term goal achievement.
HDG-MSD6: Auditing and Compliance (SF3)*	Dark data governance auditing and compliance functions are ad hoc. Limited mechanisms to gather information about dark data governance practices.	Dark data governance basic auditing processes are defined, but compliance evaluations are inconsistent. Initial sharing of audit results occurs with limited corrective actions.	Dark data governance systematic auditing and compliance evaluations are conducted regularly. Results are used to inform governance practices and drive corrective actions.	Dark data governance predictive analytics enhance auditing processes, providing real-time insights to ensure continuous compliance and accuracy in data governance.	Dark data governance adaptive auditing functions respond to new challenges, regulatory changes, and organisational needs. Continuous feedback informs proactive adjustments in governance practices.
HDG-MSD7: Adaptation (SF4)	No formal process to assess external changes. Dark data governance strategies are reactive, with minimal alignment to long-term goals.	Dark data governance initial efforts to assess external changes. Strategies are defined but lack consistency in adapting to market analysis and environmental constraints.	Dark data governance formal adaptation functions are in place, assessing external changes. Governance strategies are updated periodically to align with long-term goals.	Dark data governance predictive tools assess market trends and environmental changes. Strategies are proactively adjusted to maintain organisational adaptability.	Dark data governance fully adaptive strategies continuously respond to external changes. Long-term planning and market analysis dynamically inform governance functions to support organisational viability.
HDG-MSD8: Strategic Direction	Decision-making is isolated, with	Basic strategic direction is defined for	Strategic direction is clearly	Dark data governance advanced	Dark data governance strategic

Sub-Dimensions / Levels	Level 1: Initial (Ad-hoc)	Level 2: Developing (Defined)	Level 3: Managed (Proactive)	Level 4: Optimized (Predictive)	Level 5: Innovative (Adaptive)
and Feedback (SF5)	no formal strategic direction for dark data governance. Lack of feedback mechanisms for governance improvements.	dark data governance but not consistently applied. Limited feedback mechanisms exist to assess the alignment between current and future states.	established for dark data governance, supporting holistic context. Feedback loops exist to monitor and align governance practices with organisational goals.	decision-making processes use predictive analytics to inform strategic direction. Continuous feedback supports the dynamic alignment of governance functions.	direction is fully adaptive, balancing internal and external perspectives. Real-time feedback informs decision-making, ensuring alignment with short-term and long-term goals.

Table 5. 7 HDG-MD2 Assessment Matrix

- **HDG-MD3: Interactions of Holistic Dark Data Governance (HDG) Systemic Functions within the Organisational VSM Context**

This assessment matrix aims to characterize the maturity level of the organisation by evaluating its interactions of holistic dark data governance (HDG) systemic functions within the organisational VSM context. This HDG maturity dimension (HDG-MD3) is assessed through the following six maturity sub-dimensions (HDG-MSDs):

- **HDG-MSD9: Recursivity Levels Integration (SF6):** This systemic function integrates all governance domains (e.g. Data, IT, Corporate) within the organisation at the selected level of recursion, as well as with the organisation's external environment, to address dark data challenges. This supports the achievement of both operational and organisational objectives that are deeply embedded within the organisational system.
- **HDG-MSD10: Requisite Variety Systemic Function (SF7):** This systemic function involves both short-term and long-term data governance communications focused on identifying and addressing present and anticipated data requirements and dark data threats within the organisation's environment to achieve its goals. The holistic dark data governance system must have sufficient internal variety to effectively manage data assets and dark data risks in response to external digital disruptions and new

regulations, thereby establishing the necessary requisite variety. Identifying and responding to dark data threats and opportunities is crucial to support the organisation's goals amid external disruptions. This allows the organisation to remain agile and responsive to environmental changes at both operational and strategic levels.

- **HDG-MSD11:** Effective Inter-Operational Management (SF8): Ensures that data governance systemic functions within the organisational VSM operational units interact with coordination and control systemic functions to ensure responsive operations and sufficient autonomy with control. This enhances decision-making through self-regulation and synergy and supports the achievement of operational and organisational goals.
- **HDG-MSD12:** Metasystem Adaptability, Learning, and Change Management Systemic Functions (SF9): This represents metasystem comprising the systemic functions of control, intelligence, and corporate identity and their interaction. It provides the organisation with holistic decision-making capabilities and enables adaptability, continuous learning, and change management in data governance and dark data handling activities. The metasystem balances present and future orientations as well as internal and external perspectives, thereby supporting the achievement of both operational and organisational goals.
- **HDG-MSD13:** Communication Channels and Algedonic Channel Systemic Functions (SF10): This systemic function represents the communication channels across all data governance functions to address various types of dark data risks. For high-risk dark data scenarios that necessitate immediate intervention, algedonic channels are utilized to trigger rapid responses from operational units to top management. This ensures swift action in addressing such high-risk situations, thereby supporting the achievement of both operational and organisational objectives.
- **HDG-MSD14:** Transduction and Integration of All Systems - Common Data Governance Knowledge Systemic Functions (SF11): The integration of all systems through transduction, which facilitates a shared language across systems regarding data and dark data types, ensures cohesive operations and minimizes organisational silos. This shared understanding enhances communication between business and data stakeholders, fostering common data governance knowledge and mitigating potential dark data risks across the organisation. This, in turn, promotes organisational stability and supports the achievement of the organisation's objectives.

Table 5.8 outlines the maturity levels for the six maturity sub-dimensions of the HDG-MD3, offering organisations a structured framework to evaluate their current state and pinpoint areas for improvement in dark data governance capabilities within the organisational holistic context. This approach aims to mitigate dark data challenges and support achieving the organisation's operational and strategic objectives.

Sub-Dimension	Level 1: Initial (Ad-hoc)	Level 2: Developing (Defined)	Level 3: Managed (Proactive)	Level 4: Optimized (Predictive)	Level 5: Innovative (Adaptive)
HDG-MSD9: Recursivity Levels Integration (SF6)	No integration of governance domains (Data, IT, Corporate). Dark data challenges are addressed in isolation without considering the organisation's system as a whole.	Initial efforts to integrate governance domains exist, but they are fragmented and not consistently applied across all levels of the organisation to mitigate dark data risks	Integration of governance domains is structured and aligned with the organisation's system, addressing dark data challenges proactively.	Full integration using advanced tools and analytics. Continuous monitoring and alignment of domains with the organisation's goals and external environment to mitigate dark data risks	Adaptive integration across all domains and levels, rapidly responding to changes in both internal and external environments regarding data requirements and mitigation of dark data to meet operational and strategic goals.
HDG-MSD10: Requisite Variety Systemic Function (SF7)	No formal communication channels for identifying or addressing external dark data threats. Response to dark data requirements is reactive and disjointed.	Basic communication mechanisms are established, focusing on present data requirements. Limited response to dark data threats and external disruptions.	Proactive communication channels identify and manage current and potential dark data threats. Governance processes adapt to emerging data requirements and external regulations.	Predictive analytics and advanced communication channels anticipate and address future data threats. Systems adapt to required HDG changes dynamically, supporting long-term goals.	Fully adaptive communication channels enable rapid identification and response to dark data threats. Continuous evolution ensures resilience to external digital dark data disruptions.
HDG-MSD11: Effective Inter-Operational Management (SF8)	No interaction between HDG operational units, coordination, and control functions. Operations lack	Initial interactions between HDG operational units, coordination, and control	Defined interactions between operational units, coordination, and control,	Predictive mechanisms to enhance interactions between operational units,	Fully adaptive interaction between operational units, coordination, and control,

Sub-Dimension	Level 1: Initial (Ad-hoc)	Level 2: Developing (Defined)	Level 3: Managed (Proactive)	Level 4: Optimized (Predictive)	Level 5: Innovative (Adaptive)
	autonomy and control synergy.	functions exist but are inconsistent, limiting synergy and responsiveness to dark data risk mitigation.	fostering self-regulation. HDG Decision-making is improved through balanced autonomy and control within operations.	coordination, and control. This provides real-time insights for responsive HDG operations. Full synergy between operational units, coordination, and control of HDG systemic functions.	supporting dynamic HDG decision-making. HDG Operational autonomy and control are balanced to optimize performance and support organisational goals.
HDG-MSD12: Metasystem Adaptability, Learning, and Change Management (SF9)	No HDG adaptability or learning mechanisms with no interactions among the metasystem HDG systemic functions. Change management in dark data governance is non-existent or reactive to immediate issues.	Basic interactions among the metasystem HDG systemic functions. Basic change management processes exist, focusing on short-term adaptations. Limited efforts towards continuous learning and adaptability regarding HDG.	Established interactions among the metasystem HDG systemic functions. Established adaptability and change management processes to balance present and future HDG orientations. The organisation learns from dark data governance practices and adjusts accordingly.	HDG Predictive tools support continuous learning and adaptability. Change management processes evolve dynamically to align with both operational and strategic perspectives within the metasystem HDG systemic functions	Fully adaptive interactions within the metasystem HDG systemic functions, continuously learning metasystem. Change management strategies evolve in response to internal and external HDG feedback, ensuring organisational viability.
HDG-MSD13: Communication Channels and Algedonic Channel (SF10)	No established communication channels for addressing dark data risks. High-risk scenarios are managed reactively without structured intervention.	Basic communication channels exist but lack the efficiency and speed to manage dark data risks. Algedonic channels are partially	Effective communication channels across all data governance systemic functions to manage dark data risks. Algedonic channels	Advanced communication systems, using predictive analytics, ensure swift responses to manage dark data risks. Algedonic	Fully adaptive communication networks enable real-time intervention to manage dark data risks. Algedonic channels seamlessly

Sub-Dimension	Level 1: Initial (Ad-hoc)	Level 2: Developing (Defined)	Level 3: Managed (Proactive)	Level 4: Optimized (Predictive)	Level 5: Innovative (Adaptive)
		implemented for some high-risk situations.	trigger rapid responses for high-risk dark data situations.	channels dynamically adjust to address varying levels of dark data risk.	integrate to address high dark data risks and support operational and strategic objectives.
HDG-MSD14: Transduction and Integration of All Systems (SF11)	No common language or understanding of data types or dark data types across the organisation. Dark data governance is fragmented, leading to organisational silos.	Initial transduction processes are in place, but integration across HDG systemic functions is limited. HDG Communication and HDG common knowledge between business and data stakeholders is inconsistent.	Structured transduction facilitates shared language and cohesive operations regarding dark data management. Common dark data governance knowledge reduces organisational silos and addresses dark data risks.	Advanced transduction integrates all HDG systemic functions. Predictive analytics enhance cohesive operations and common knowledge between stakeholders.	Fully adaptive transduction and integration among HDG systemic functions, promoting organisational stability. Common dark data governance knowledge that supports operational and strategic goals.

Table 5. 8 HDG-MD3 Assessment Matrix

5.5.2. Structure of Implementing and Utilizing the Assessment Matrix

The assessment matrix for holistic dark data governance is a valuable tool for evaluating and enhancing the implementation of dark data governance within organisations. It is a practical instrument designed to support the deployment of dark data governance systemic functions within the organisation's Viable System Model context. This section aims to outline the structure and application of the assessment matrix. Implementing the assessment matrix will yield insights into the overall maturity level of holistic dark data governance in organisations. To implement and utilize the holistic dark data governance assessment matrix, the assessment criteria will be developed based on the content of this matrix, and the assessment results may be presented visually. These criteria will be used as statements provided to organisations to evaluate the maturity levels of their holistic dark data governance, based on the defined dimensions. The statements are derived from the content of the assessment matrix for each sub-dimension.

The assessment process begins by evaluating multiple statements to assess the maturity of each sub-dimension. The overall maturity level for the holistic dark data governance in the organisation will be based on the 14 core maturity sub-dimensions. Figure 5.7 outlines the high-level architecture to implement and use the holistic dark data governance assessment matrix.

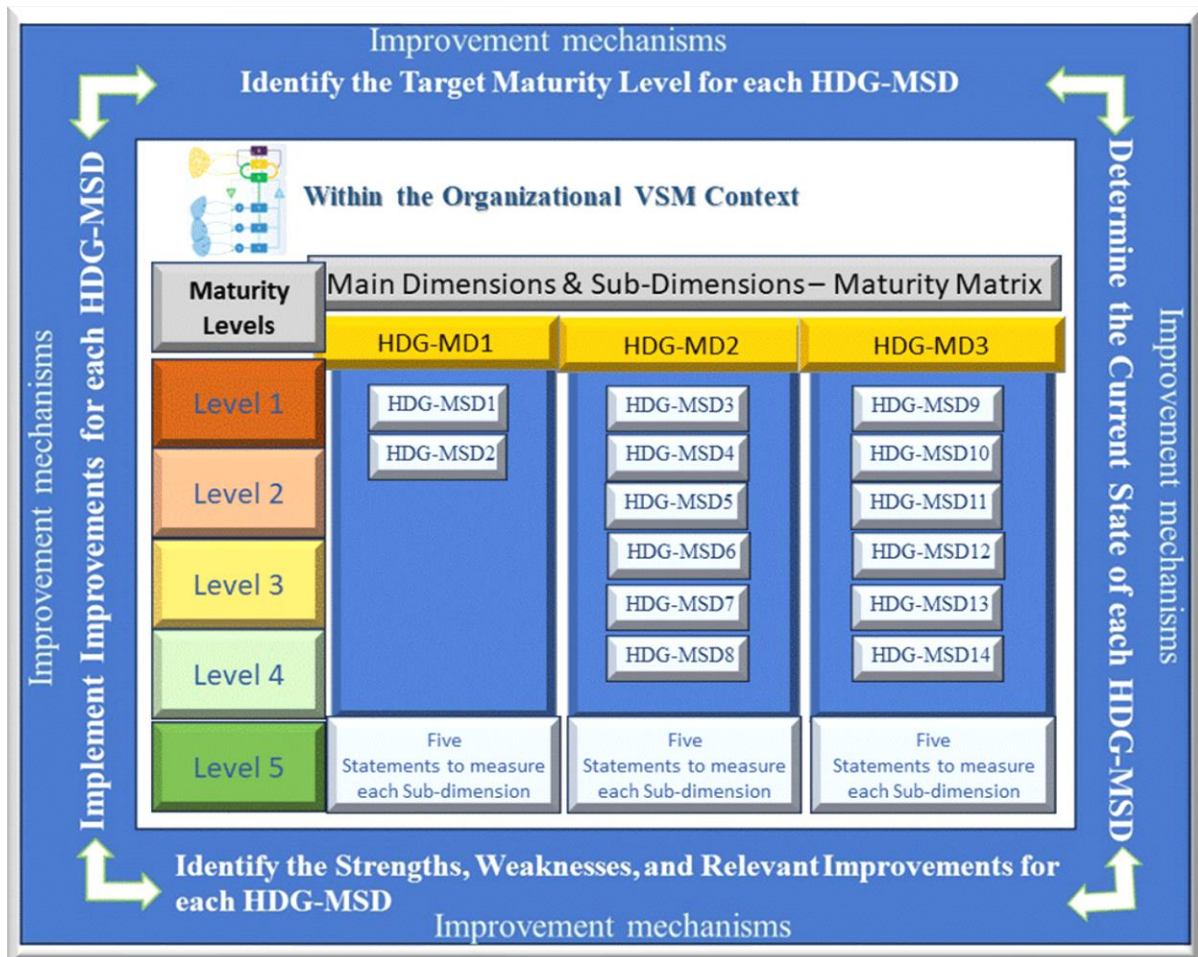


Figure 5. 7 The structure to implement the holistic dark data governance assessment matrix.

5.6. Chapter Summary

This chapter presents the holistic dark data governance maturity model and an associated assessment matrix. The literature review revealed that existing maturity models have been developed either based on the Capability Maturity Model (CMM) or the conceptual construction of the topic. Accordingly, the maturity model developed in this research employed conceptual construction as a theoretical foundation. The maturity model comprises three key components: an improvement mechanism, maturity levels, and dimensions. The dimensions represent the essential elements of the holistic dark data governance model required to design,

deploy, and sustain effective dark data governance systemic functions, as discussed in Chapter 4. This chapter outlines the aims and motivation behind the maturity model and then describes the dimensions used to assess the maturity of dark data governance within an organisation. The chapter also defines and discusses the maturity levels and their relationship to the dimensions of the model. The research adopted a systematic methodology for developing the holistic dark data governance maturity model, encompassing three phases: Pre-Design, Design, and Post-Design, each with multiple tasks to achieve the intended objectives. Regarding the assessment matrix, this chapter explains the development process and the implementation approach, which utilizes statements to describe the current state of the holistic dark data governance dimensions within the organisation. Finally, this chapter outlined the structure for implementing and using the holistic dark data governance assessment matrix. The following chapter will present and discuss the validation of the holistic dark data governance model.

Chapter 6. Validation of the Holistic Dark Data Governance Model

6.1. Introduction

Validating the framework/model is a crucial component of the development process, as it reinforces confidence in the framework/model and enhances its utility ([Kennedy, W., 2005](#)). Validation can be described as the process of assessing the degree to which a model accurately represents the real world from the standpoint of the intended applications of the model ([Oberkampff, L. W. and Trucano, T., 2008](#)). Validating the dark data governance framework is crucial to ensure the proposed model adequately addresses the key factors for successfully mitigating dark data and achieving organisational goals. This chapter delves into the validation of the dark data governance model, exploring the various approaches and techniques employed to assess its accuracy and applicability. The assessment of the model's accuracy and applicability in representing reality will be informed by expert evaluation. Prior studies have employed a variety of methods to validate frameworks and models, including surveys, case studies, questionnaires, focus groups, interviews, and workshops ([Kennedy, W., 2005](#)); ([Oberkampff, L. W. and Trucano, T., 2008](#)); ([Martínez, F. A. and Largo, L. F., 2009](#)). In this research, the proposed model was validated through a Delphi Study for the case of a key university in Texas, USA.

6.2. Design of the Validation Approach

The motivation of this thesis was to support key universities in Texas, USA deploying an effective holistic dark data governance model, therefore the outcomes of the research were validated in this chapter. The Delphi method was selected as the appropriate technique to validate the model since it is well-suited for eliciting expert opinions and reaching a consensus on complex issues ([Sargent, G. R., 2013](#)). The Delphi method involves a panel of experts who participate in a series of iterative questions, with the results of each round fed back to the panel to refine and elaborate further on their responses in subsequent rounds([Sargent, G. R., 2013](#)). The Delphi technique has several advantages for validating the proposed framework, as it allows for ([Omar, A. and Almaghthawi, A., 2020](#)):

- Anonymity of participants to reduce potential bias
- Controlled iterative feedback to encourage reflection and refinement of opinions through a series of questions centred around a key subject (in our study, it is holistic data governance)
- Aggregation of individual judgments into the most reliable group consensus

The Delphi technique is a research method commonly used in the field of data governance ([Kim, H, D., 2024](#)). It involves gathering input from a group of experts through multiple rounds of questionnaires or surveys, with the goal of reaching a consensus or understanding on a particular topic or issue ([Baker, S., Edwards, R. and Doidge, M., 2012](#)). This approach allows for the integration of different perspectives and expertise, ensuring a comprehensive and well-rounded examination of the subject matter. Furthermore, the Delphi technique allows for the anonymity of participants, eliminating power dynamics that may influence their responses. This method of controlled interaction among participants represents a deliberate effort to mitigate the drawbacks associated with more traditional methods of gathering expert input, such as round-table discussions or other less structured forms of engaging with differing perspectives.

Additionally, the Delphi technique provides a systematic and iterative approach to data collection and analysis, allowing for refinement, building up on ideas, and consensus-building among experts. By utilizing the Delphi technique, the researcher can tap into the collective wisdom and expertise of participants to generate a comprehensive and holistic understanding of data governance ([Patunob, B, G. and Ibojo, M, T, D., 2023](#)) and make informed decisions in their research ([Ragab, M. and Arisha, A., 2017](#)). This approach is particularly beneficial for a PhD research on holistic data governance, as it allows the researcher to gather insights from a wide range of perspectives and validate their findings through a structured and iterative process ([Baker, S., Edwards, R. and Doidge, M., 2012](#)) to data collection and analysis ([Mohammed, A, A., 2023](#)). By utilizing the Delphi technique for holistic data governance, the researcher can gather insights and recommendations from a diverse group of experts to inform their study and contribute to the development of knowledge in the field of holistic data governance ([Hu, H. and Yan, H., 2013](#)). The process of conducting Delphi research involved several steps ([Gale, N. et al., 2013](#)). The first step was to select a panel of experts who possess relevant knowledge and expertise in the field of data governance, IT governance and governance at large. The panel of experts for our case study involved thirteen (13) participants, all of whom have good experience related to governance.

The selected experts came from diverse backgrounds and disciplines to ensure a comprehensive examination of dark data governance. The next step was to create a questionnaire or survey that was used to gather input from the experts. The questionnaire was carefully designed to elicit detailed and informed responses from the experts, capturing their insights, opinions, and recommendations related to holistic data governance ([Baker, S., Edwards, R. and Doidge, M., 2012](#)). The following step in the Delphi research process was to distribute the questions at high

level to the panel of experts and allow them sufficient time to provide their responses. The researcher (Author) also provided clear instructions and guidelines for completing the questions to ensure consistency in the responses (Gale, N. et al., 2013). Furthermore, the Delphi technique involved conducting multiple rounds (3 rounds) of data collection for different levels of details and analysis ([Baker, S., Edwards, R. and Doidge, M., 2012](#)). The Author analysed the responses received in each round, identified areas of agreement and disagreement among the experts, and summarized their findings ([Gale, N. et al., 2013](#)). Based on the analysis, the Author created more elaborate questions for the next round of data collection, incorporating the feedback and insights from the previous round of experts. This iterative process continues until a consensus or convergence of opinions was reached among the panel of experts regarding holistic data governance after the 3rd round. Once a consensus was reached, the Author then interpreted and analysed the findings to generate the final validated version for holistic data governance model. The consensus was 60% and above for the panel's findings to be considered valid and reliable. Furthermore, the Delphi technique allowed for the identification of areas of agreement and disagreement among experts, which can inform future research and policy-making in the field of holistic data governance ([Baguley, I. et al., 2014](#)).

This study highlights the importance of involving diverse perspectives and expertise in the development of data governance practices ([Bargagliotti, E. A. et al., 2020](#)). By utilizing the Delphi technique, the researcher was able to gather insights and reach a consensus on the key elements and best practices for holistic data governance from a panel of experts with varied backgrounds and experiences ([Omar, A. and Almaghthawi, A., 2020](#)) ([Benfeldt, O., 2017](#)) ([Yusuwan, M. N. et al., 2021](#)). The iterative and anonymous nature of the Delphi technique also helped to reduce potential biases and power dynamics that may influence the responses, ensuring a more objective and well-rounded assessment of the topic ([Sourani, A. and Sohail, M., 2014](#)). Additionally, the structured and systematic approach of the Delphi method allowed for the refinement and building upon of ideas, ultimately leading to a more comprehensive and validated model for holistic data governance ([Kache, F. and Seuring, S., 2017](#)). The population for this study, as with all Delphi studies, is a selection of experts in a respective field (data governance, IT governance, and governance at large) that have the experience and knowledge that will provide reliability and validity to this study ([Giannarou, L. and Zervas, E., 2014](#));([Dalkey, C. N. and Helmer, O., 1962](#)).

6.3. Panel of Experts Validation Scope

The scope of the validation by the panel of experts was based on three tasks: focus on this study's research problem, describe the panel feedback including analysis of the validation results, and update the proposed model of dark data governance after validation by the participants where consensus is at least 60% - as elaborated in the following three sections below.

6.3.1. Research Problem vs. Validation Scope of the Proposed Model

The proposed Holistic Dark Data Governance Model (HDGM) addresses the key research questions of this study regarding dark data governance. For RQ1, it tackles the formal and informal components adopted by organisations to manage and govern dark data, conceptualized through dark data HDG systemic functions within the VSM context and validated in this Chapter. RQ2 examines the impact of aligning data governance with other governance domains across different management levels and functions, conceptualized through the model's context and design and validated in this Chapter. RQ3 investigates the emphasis on key data governance concepts within organisations, particularly in managing various types of dark data (high risks vs. other types), conceptualized through systemic function SF10 and validated in this Chapter. Table 6.1 illustrates the research questions of this study versus the proposed dark data HDG model and its validation process.

Research Questions (of this Study)	Proposed HDGM	Validation Scope
RQ1: What are the key components of dark data governance (both formal and informal) that organisations adopt to manage the power and impact of various types of dark data?	Covered under dark data HDG systemic functions of the model for each systemic element within the VSM context (in an organisation)	Validation covered in Round-1 and Round-2 Questions
RQ2: How has the holistic data governance context affected the management of dark data? Holistic context: alignment of DG with other relevant governance domains (ex: IG, DM, IT Governance) across the locations of decision-making authorities (executive management, middle management, and operational level) within the different functions (ex: business, IT)	Covered under dark data HDG model context and design (in an organisation)	Validation covered in Round-1, Round-2, and Round-3 Questions

Research Questions (of this Study)	Proposed HDGM	Validation Scope
RQ3: Within the holistic data governance context, do the key DG concepts have similar emphasis within organisations in managing the different types of dark data?	Covered under dark data HDG SF10 (within an organisation)	Validation covered in Round-2 Questions

Table 6. 1 Research questions versus the validation Scope of the Proposed Model

6.3.2. Experts' Feedback Description and Analysis

The feedback data was collected in three rounds using a systematic and iterative approach to data collection and analysis. This method allowed for refinement, the building up of ideas, and consensus-building among experts, as described in Section 6.2. This work was achieved as follows:

- Conducted awareness training sessions on the HDG Model to ensure comprehensive understanding and provide necessary clarification on the model throughout the data collection process. These sessions throughout the process also helped rectify questions in the three rounds (Appendix N) as needed to ensure clarity and sign the relevant ethical forms (Appendix B).
- Distributed the Round 1 questions to validate the proposed model by:
 - Validating the HDG model's systemic design within the VSM context, ensuring its effectiveness in counteracting dark data and supporting the achievement of organisational goals. Closed questions with a five-point Likert scale were used to gather participants' feedback.
 - Validate the HDG model's key systemic phases within the organisational VSM context, focusing on its ability to address dark data and support organisational goals. Closed questions with a five-point Likert scale were utilized to execute this step.
 - Obtaining suggestions from participants to improve the holistic dark data governance model to counteract dark data and support the achievement of organisational goals. Open questions were utilized to identify areas for improvement to refine the model's key systemic phases as necessary.
- Distribute the Round 2 questions to further validate the proposed model by:
 - Refining and validating questions and responses from Round 1 as necessary

- Building upon the key phases from Round 1 to validate the HDG systemic functions of the model under each systemic phase within the VSM context, with a focus on counteracting dark data and supporting the achievement of organisational goals. Closed questions with a five-point Likert scale were utilized to execute this step.
- Obtaining suggestions from participants to improve the holistic dark data governance model to counteract dark data and support the achievement of organisational goals. Open questions were utilized to identify areas for improvement to refine the model's key systemic functions for each phase as necessary.
- Distribute the Round 3 questions to validate the proposed model by:
 - Refining and validating questions and responses from Round 2 as necessary
 - Validate the usability of implementing the HDG model within the organisational VSM context to counteract the dark data and support the achievement of organisational goals.
 - Refining and validating questions and responses on the proposed model from Round 3 as necessary
- Performing content analysis of the collected data and ensuring at least a 60% consensus among participants. Based on the recommendations and validation results from the panel of experts, defining the improvements and updates to be made to the proposed model, ensuring the changes reflect an expert consensus of 60% or above.
- Updating and improving the proposed HDG model to produce the final version of the model, as elaborated in Section 6.5.7.

6.3.3 Deliverables

A deliverable in this context is any unique and verifiable result of the feedback provided by the panel of experts, where at least 60% consensus is achieved. This feedback details the necessary changes and improvements required to complete a context, model objective, model design, or model phases and phase systemic functions. The deliverable within this stage allowed for improvements and updates to be made to the proposed model, driven by the recommendations and results of the validation provided by the panel of experts with at least 60% consensus.

6.4. Participant Profiles

The panel of experts included thirteen participants (coded P1 to P13) from a key university (size > 5,000) in Texas, USA. Participants were selected based on their homogeneity in education and recent experience with data governance, Information Technology (IT) governance, and governance in general. The data collection process aimed to gather feedback from various departments across different management levels simultaneously. This approach ensures a comprehensive understanding of perspectives and experiences, enhancing the reliability and depth of the feedback obtained. Table 6.2 presents the demographic characteristics of the participants, detailing their roles, years of experience in their current positions, data governance experience, and overall governance experience. The participants hold diverse roles such as Data Governance Manager, IT Manager, President, Vice President, Director, Senior Analyst, Professor, Researcher, and Student. They possess significant experience in their current positions, ranging from 4 to 15 years, and have substantial experience in data/IT governance, spanning 3 to 11 years, as well as overall governance experience ranging from 1 to 11 years. This indicates a well-rounded and experienced group of participants.

Participant Code	Role	Experience in Current Job	Data/IT Governance Experience	Governance Experience
P1	President	15 years	5 years	11 years
P2	Data Governance Manager	13 years	11 years	7 years
P3	IT Manager	10 years	7 years	5 years
P4	Vice President	12 years	4 years	10 years
P5	Director of Data Governance	11 years	10 years	10 years
P6	Data Governance Senior Analyst	10 years	9 years	3 years
P7	Director of Learning & Development	7 years	4 years	5 years
P8	Professor – Graduate School	8 years	4 years	3 years
P9	Researcher	9 years	5 years	2 years
P10	Student – Graduate School	4 years	3 years	1 year
P11	Data Governance Coordinator	9 years	7 years	3 years
P12	Professor Undergraduate School	10 years	5 years	3 years
P13	Student - Undergraduate School	4 years	3 years	1 year

Table 6. 2 The demographic characteristics of the participants

6.5. Data Analysis

The Author employed both quantitative and qualitative data analysis techniques to validate the proposed framework, leveraging the participants' feedback. The quantitative component involved the use of a five-point Likert scale to assess the validation criteria, including the model design, model elements, systemic functions of the model, and usability. Regarding the qualitative feedback, the validation process included open-ended statements, which allowed the participants to provide a rationale for their opinions and offer additional comments and recommendations to refine and enhance the model. It was essential to strike a balance between the validation results and the participants' suggestions to ensure the proposed framework could be more effectively implemented across various universities and organisations. The data analysis process involved a systematic approach to synthesize the quantitative and qualitative feedback from the expert panel, with the goal of producing a comprehensive and validated model for holistic data governance that could be broadly adopted. Figure 6.1 illustrates the convergence point to develop a reliable and valid model.

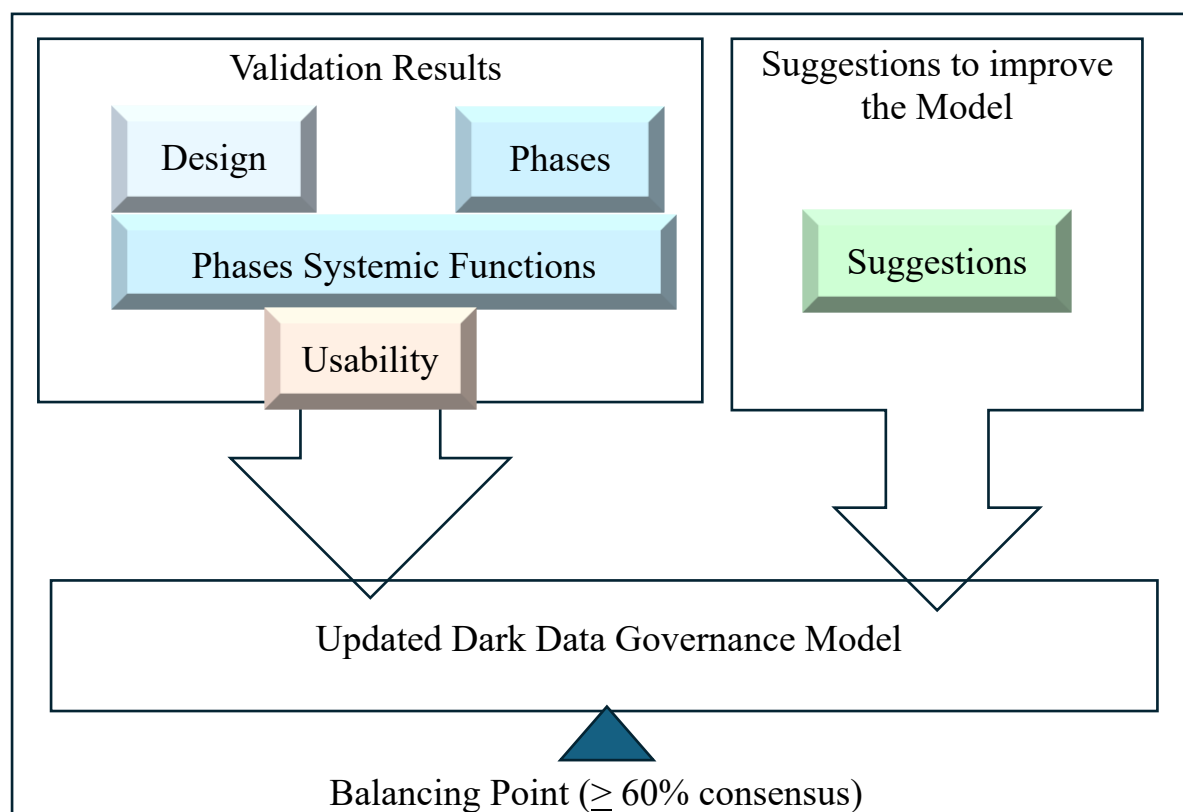


Figure 6. 1 The balancing point for the accuracy of the framework

6.5.1. Proposed Model Design Validation

This step aims to examine whether the model design meets the research goals and objectives. It includes ten statements, coded St 1.1 to St 1.10, in which participants used a Likert scale from 5 (strongly agree) to 1 (strongly disagree) to indicate their agreement or disagreement with each statement, thereby rating the framework's design versus the research objectives. The consensus of the participants' feedback on the statements to validate the model design is illustrated in Table 6.3 And Figure 6.2.

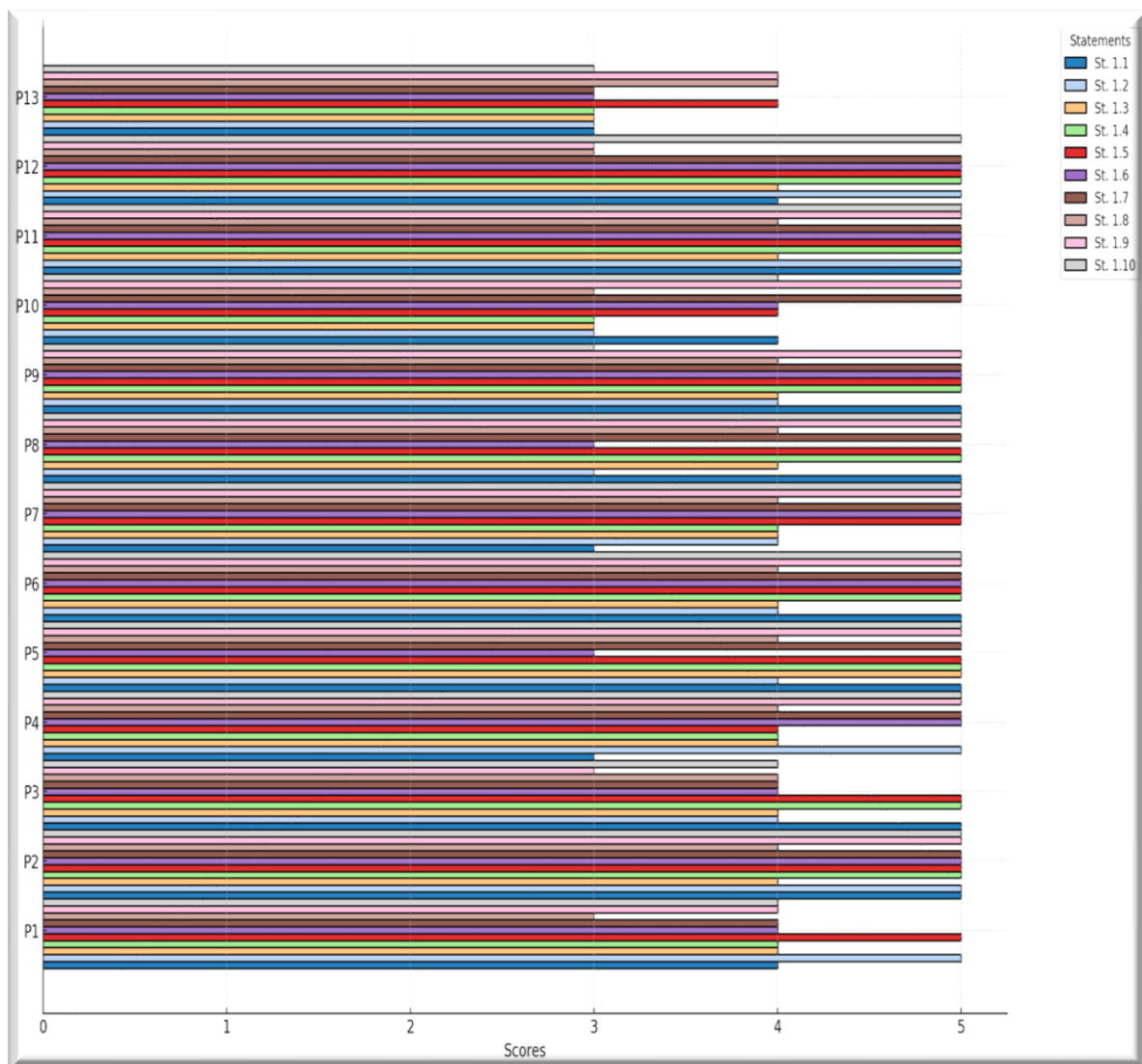


Figure 6. 2 The participants' feedback on the validation statements of the model design

This graph summarizes the ratings given by each participant regarding the holistic dark data governance model design for each statement and each participant.

St. 1.n	Description	% of Consensus	Mean
St. 1.1	The model provides a methodology to deploy, assess, and sustain an effective holistic dark data governance model.	79	4.31
St. 1.2	The model provides a structured methodology for supporting decision-makers to understand important systemic functions to deploy, assess, and sustain dark data governance subsystems within an organisational context.	79	4.15
St. 1.3	The model supports organisational continuous learning, corporate harmonization, and change management in handling dark data issues and achieving organisational goals.	79	3.92
St. 1.4	The model ensures effective and responsive operational units by balancing autonomy with control through coordinated data governance activities. This supports decision-making and the achievement of operational and organisational goals.	86	4.46
St. 1.5	The model supports adaptability and the achievement of long-term goals by effectively addressing dark data constraints and leveraging data opportunities	99	4.73
St. 1.6	The Model establishes, evaluates, and enhances corporate holistic data governance policies, ensuring a consistent operational framework to counteract dark data. It balances dark data governance internal and external perspectives to support the achievement of the current and future goals.	79	4.31
St. 1.7	The Model manages the complexity of the environment by responding to digital data disruptions and emerging data and data governance regulations. This enables the organisation to remain agile in achieving its goals and maintain stability.	93	4.69
St. 1.8	The model will help organisations to reduce the cost, time, and effort involved in counteracting dark data and achieving its goals.	71	3.77
St. 1.9	The model ensures accuracy and compliance with data governance standards, supporting corrective actions and achievement of the organisational goals.	86	4.54
St. 1.10	The model has immediate interventions to ensure organisational goal achievement and rapid response to high dark data risks.	86	4.46

Table 6. 3 The consensus and means of the participants' feedback on the statements to validate the model design

This table summarizes the descriptions for each statement regarding the design of the holistic dark data governance model along with the percentage of the consensus and the mean rating for the participants' feedback on each statement. The analysis shows strong consensus on the effectiveness of the holistic dark data governance model across all statements. The model is particularly appreciated for providing a structured methodology, supporting decision-making, ensuring operational effectiveness, supporting long-term adaptability, managing environmental complexity, reducing costs, ensuring accuracy and adherence to standards, and providing immediate interventions for high-risk scenarios. Overall, the feedback indicates strong consensus and positive ratings for the holistic dark data governance model, with most statements achieving a high percentage of consensus and a mean rating above 4.0.

In Figure 6.3, the blue bars represent the mean ratings for each statement, and the green line with markers indicates the percentage of consensus for each statement. The solid red line represents the 60% consensus threshold. This visualization effectively highlights the consensus threshold along with the ratings and consensus levels for each statement.

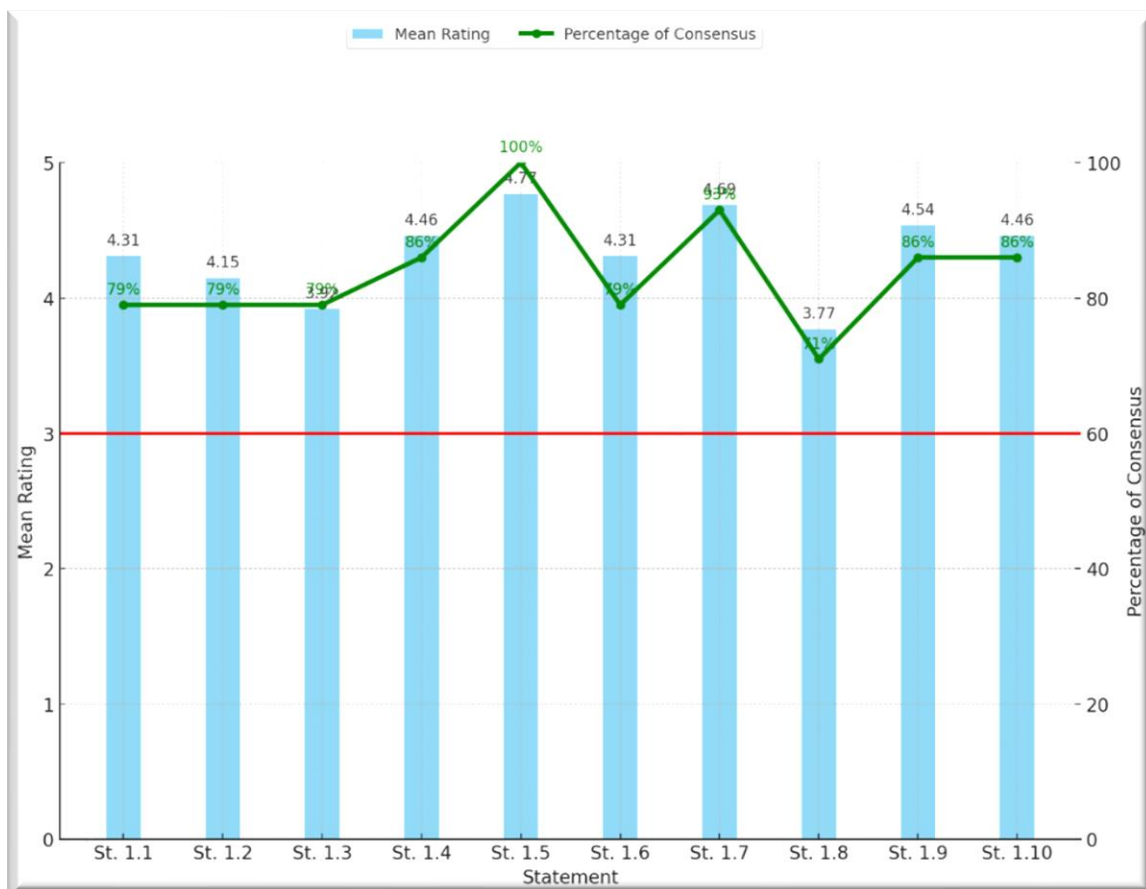


Figure 6. 3 The consensus and means of the participants' feedback on the statements to validate the model design

The holistic dark data governance model is highly regarded by participants, with most statements receiving mean ratings above 4.0 and strong consensus. The highest approval is for the model's support for adaptability and long-term goals, with a mean rating of 4.77 and 100% consensus. Participants also strongly agree on the model's effectiveness in managing complexity, as shown by a mean rating of 4.69 and 93% consensus. While there is overall satisfaction, the model could improve in reducing costs, time, and effort, as indicated by the lowest rating of 3.77 for that aspect. Overall, the model is seen as effective in supporting decision-making, ensuring operational effectiveness, and providing immediate interventions for high-risk scenarios.

6.5.2. Model Systemic Phases Validation

The goal of this step is to determine whether the participants agree with the model's systemic phases in terms of whether these phases support important systemic functions (SFs) and increase understanding of dark data governance requirements. This step comprises three phases, which were coded Phase 1 to Phase 3. A Likert scale of importance from 5 (very important) to 1 (not important) was used to indicate the participants' feedback to each phase and to rate the phases of the model. Figure 6.4 shows the participants' feedback on these statements.

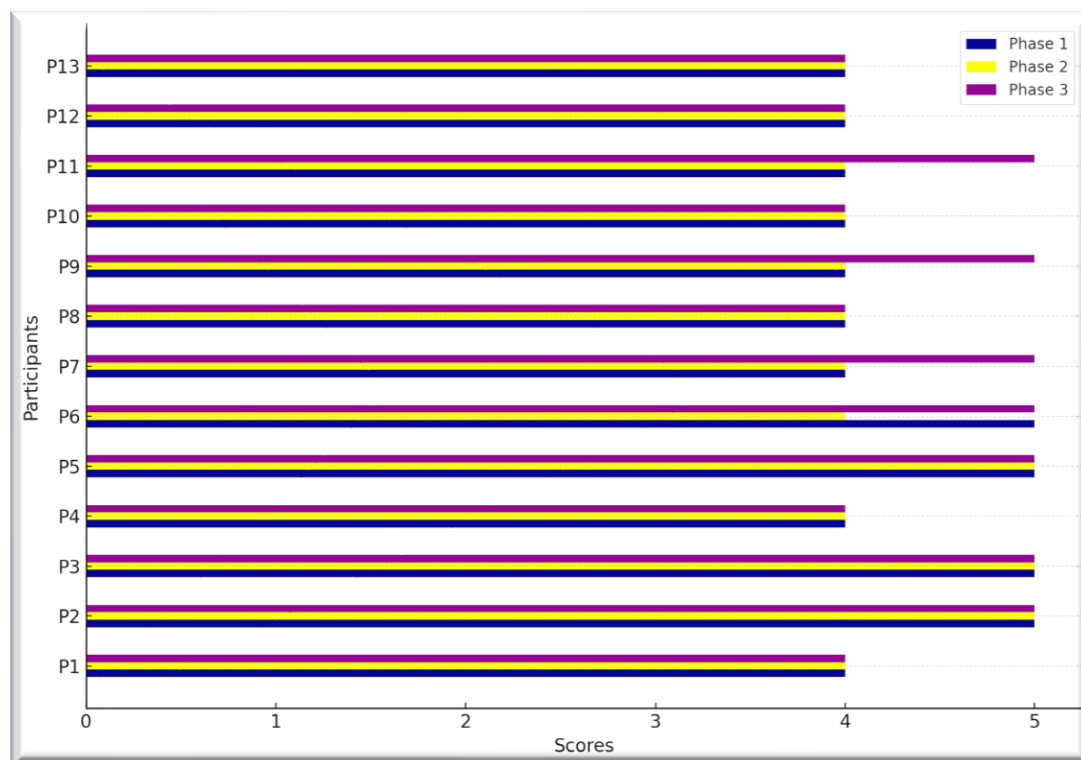


Figure 6. 4 The participants' feedback on the validation of the model phases

The above graph displays the scores for each phase of each participant. Each bar represents the score of importance for a particular phase, color-coded for clarity. The participants are listed on the y-axis, and their scores are on the x-axis. This visualization compares the ratings of each phase by different participants side by side.

Table 6.4 summarizes the feedback on the importance of the three systemic phases of the Holistic Dark Data Governance Model (HDGM). The ratings for each phase by various participants, along with the consensus percentage and mean rating, has been generated. Each phase has achieved more than 60% consensus, indicating strong agreement among participants on the model phases.

Phase ID	Phase Description	Consensus %	Mean
Phase 1	Contextualize HDGM: Identifying the organisational system-in-focus within the Viable System Model is vital to contextualize, assess, and sustain the holistic data governance model (HDGM) as a subsystem within the system-in-focus. This is crucial to identify the organisation's goals and objectives and the goals of the holistic data governance model to mitigate dark data risks and support organisational viability and goal attainment.	92%	4.31
Phase 2	HDGM Key Systemic Functions: Identifying, deploying, assessing, and sustaining the systemic functions of the holistic data governance model (HDGM) within the five subsystems of the Viable System Model is essential to counteract dark data and support the achievements of the organisational objectives. This is crucial to deploy, assess, and sustain the corporate policies developed for key data governance domains, as well as harmonization, cohesion, autonomy, auditing, compliance, adaptation to the environment, and the overall data governance direction to ensuring a balance between current and future functions.	85%	4.23
Phase 3	Key Interactions among HDGM Systemic Functions: Identifying, deploying, assessing, and sustaining the key interactions among the holistic data governance systemic functions (HDG SFs) within the five subsystems of the Viable System Model is essential to counteract dark data and support the achievements of the organisational objectives. This integrated approach with IT and corporate governance is crucial to governing data assets, addressing dark data risks arising from external disruptions, identifying dark data types, promoting	95%	4.54

Phase ID	Phase Description	Consensus %	Mean
	organisational agility in handling dark data risks, enhancing decision-making, balancing the holistic data governance model's present and future orientations as well as internal and external perspectives, support learning and change management, and enable immediate interventions in high-risk dark data situations.		

Table 6. 4 The consensus and means of the participants' feedback on the validation of the model phases

Figure 6.5 is the graph with two y-axes: one for the mean scores and one for the consensus percentages. The mean scores are displayed as bars, while the consensus percentages are shown as a red line with markers. This visualization allows for a clear comparison of both mean ratings and consensus on the importance across the three phases.

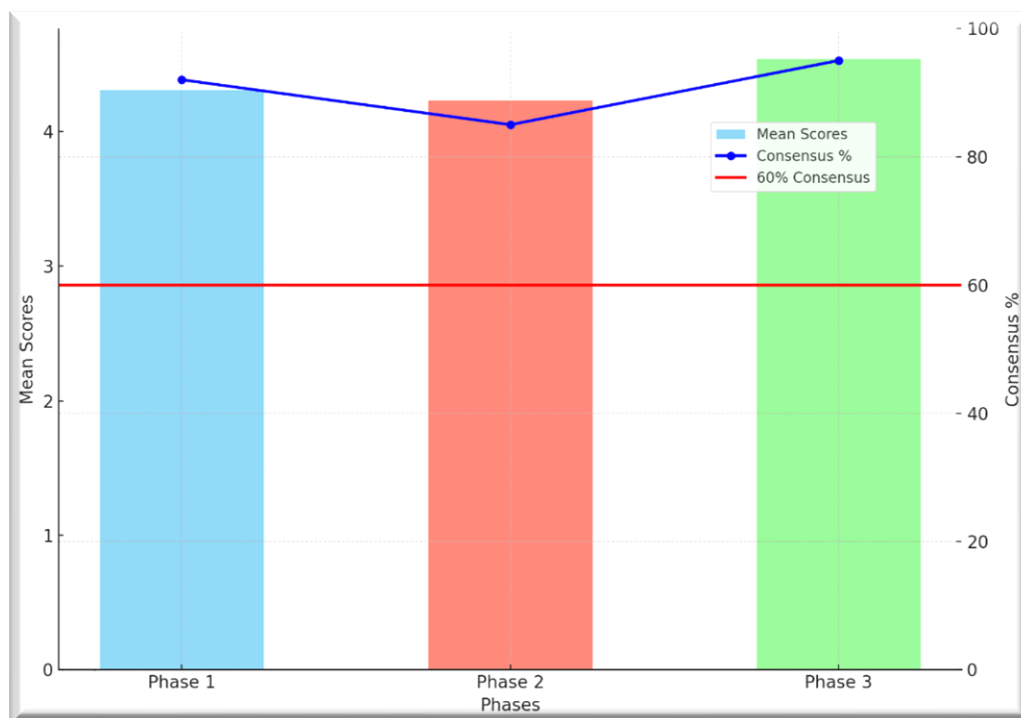


Figure 6. 5 The participants' feedback on the validation of the model phases

The feedback in Figure 6.5 indicates strong support for all three phases of the HDGM systemic model, with each phase achieving high consensus (> 60%) and mean scores.

The participants recognize the importance of contextualizing the HDGM within the organisational system, deploying and sustaining key systemic functions, and ensuring effective interactions among these functions to counteract dark data risks and support organisational

goals. The highest support is observed for Phase 3, highlighting the critical role of integrated governance and agility in handling dark data. The results show that the participants indicated that all the systemic phases were important with consensus above 60%.

6.5.3. Validate the Systemic Functions Components of the Model Phases

In the previous section, the model phases in general have been validated; thus, this section aims to validate the components in these phases. This section used a Likert scale of importance from 5 (very important) to 1 (not important) to indicate the participants' feedback on each systemic function to rate each component in the model framework phases.

- **Validation Results of Phase 1 - Contextualize HDGM**

This step aims to validate the first phase components to make sure that these components are important when identifying the significant requirements for deploying, assessing, and sustaining the model. Phase 1 includes two systemic functions as components, coded SF 1.1 and SF 1.2. Figure 6.6 shows the participants' feedback on these SFs.

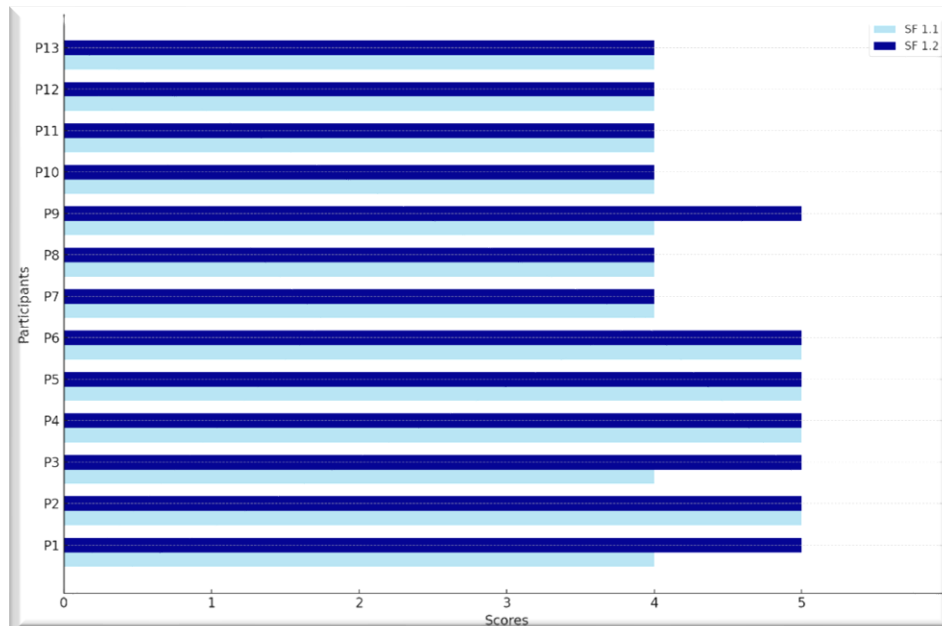


Figure 6. 6 The participants' feedback on the SFs of Phase 1

The graph presents the participants on the y-axis and scores on the x-axis. The bars are coloured in light blue and dark blue, representing the scores for each systemic function. This

visualization compares the ratings of each phase by different participants side by side. Table 6.5 shows the mean and consensus percentage of the participants' feedback.

SF ID	Systemic Function (SF) Description	Mean	Consensus %
SF 1.1	Identify the organisational VSM system-in-focus (Organisational level) with its purpose, goals, stakeholders, and boundaries of the organisation within its environment. Define dark data governance purpose. Dark Data governance purpose for this study is to counteract dark data risks and create business value to support organisational viability and goal achievement.	4.31	86.2%
SF 1.2	Contextualize, deploy and sustain the scope to support the goals of the holistic data governance model (HDGM) as a subsystem within the organisational VSM system-in-focus. The goal is mainly to counteract dark data risks and support organisational viability and goal achievement.	4.54	90.8%

Table 6. 5 The mean and consensus% of the participants' feedback on the SFs of phase 1

Table 6.5 summarizes the feedback on the importance of the two systemic functions (SFs) in Phase 1 of the model. The table presents the ratings provided by various participants for each SF, along with the consensus percentage and mean rating. Both SFs achieved more than 60% consensus, indicating strong agreement among participants on their importance in Phase 1. Figure 6.7 shows mean scores and consensus percentages as a graph.

Figure 6.7 is the graph with two y-axes: one for the mean scores and one for the consensus percentages. The mean scores are displayed as bars, while the consensus percentages are shown as a green line with a 60% threshold marked by a red line. This visualization allows for a clear comparison of both mean ratings and consensus on the importance across the two SFs.

The analysis shows a high level of agreement among participants on the importance of both systemic functions (SF 1.1 and SF 1.2) within phase 1 of the HDGM. The ratings indicate that participants recognize the need to clearly define the organisational VSM system-in-focus and to contextualize, assess, and sustain the goals of the holistic data governance model. The mean scores of 4.31 for SF 1.1 and 4.54 for SF 1.2, with corresponding percentages of 86.2% and 90.8%, reflect a strong consensus on the value of these functions in supporting organisational viability and goal achievement by addressing dark data risks.

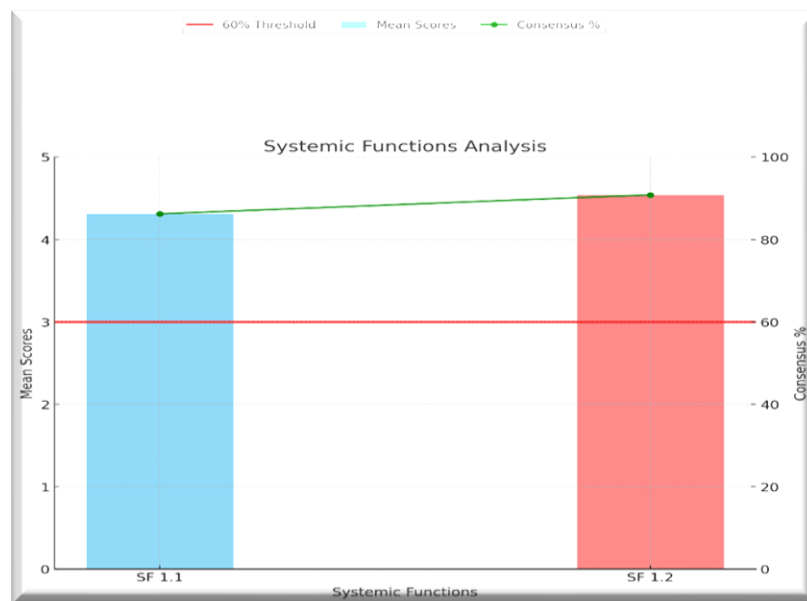


Figure 6. 7 The participants' feedback on the validation of the SFs of Phase 1

● Validation Results of Phase 2

This step aims to validate the second phase components to make sure that these components are important when identifying the significant requirements for deploying, assessing, and sustaining the model. Phase 2 includes six systemic functions as components, coded SF 2.1 to SF 2.6. Figure 6.8 shows the participants' feedback on these SFs.

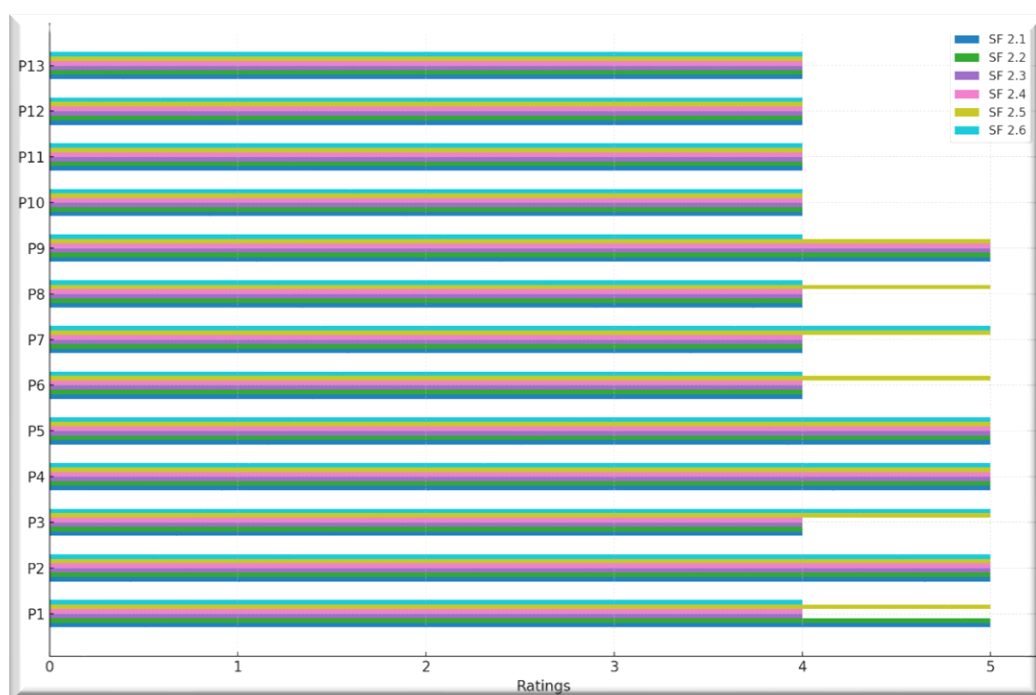


Figure 6. 8 The participants' feedback on the SFs of Phase 2

The graph presents the participants on the y-axis and scores on the x-axis. The bars represent the scores for each systemic function in phase 2. This visualization compares the ratings of each SF by different participants side by side. Table 6.6 shows the mean and consensus percentage of the participants' feedback.

SF ID	Systemic Function (SF) Description	Mean	Consensus %
SF 2.1	HDG SF1 Support to Operational Units (HDG SF1 within VSM S1) - identify the primary activities that deliver the organisational products or services. Deploy, and sustain HDG policies, guidelines, and procedures, to provide core activities with necessary data and counteract dark data risks. HDG SF1 supports organisational viability and the achievement of operational goals.	4.38	88%
SF 2.2	HDG Harmonisation (HDG SF2 within VSM S2): Define, deploy, and sustain compliance with corporate dark data governance systemic functions (e.g. corporate policies, guidelines, standards, rules, and protocols) to prevent recurrent dark data governance conflicts and misalignment among primary units within S1. Deploy identified corrective actions and continuously improve as appropriate to support corporate harmonization. HDG SF2 supports organisational viability and the achievement of operational goals.	4.38	88%
SF 2.3	HDG Cohesion & Autonomy (HDG SF3 within VSM S3): define, develop, and sustain corporate dark data governance systemic functions: HDG Corporate policies, HDG performance measurements, HDG compliance requirements, HDG resource requirements (e.g. Technology, Financials, competencies) requirements, and allocation of HDG resources to SF1. Corporate policies are developed for key data governance domains: Data Architecture, Data Quality, Metadata, Data Security, Reference & Master Data, Data Warehousing/Business Intelligence/Artificial Intelligence, Data Modelling & Design, Document & Content Management, Data Storage & Infrastructure/Operation, Data Integration & Interoperability. HDG SF3 supports the balance between self-regulation (Autonomy) for each operational unit in S1 and their synergies (Cohesion) amongst them for improved organisational performance and achievement of operational and organisational goals.	4.31	86%
SF 2.4	HDG Audit and Compliance (HDG SF3* within S3*): Conduct, deploy, and sustain data governance auditing and compliance	4.31	86%

SF ID	Systemic Function (SF) Description	Mean	Consensus %
	functions to gather information about data requirements and dark data challenges from S1 units. Accordingly, results and improvements are shared through key communication channels among SF3, SF3*, and SF1. This is to support the achievement of organisational goals.		
SF 2.5	HDG Intelligence /Adaptation (HDG SF4 within S4): Conduct research, development, and corporate planning to make sense of the environmental changes such as constraints and opportunities related to data needed by the organisation and potentially encountering dark data that could threaten organisational viability. Deploy, and sustain the holistic data governance strategy and long-term orientated tasks to support and improve the adaptability and the achievement of the organisation's long-term goals.	4.69	94%
SF 2.6	HDG Policy, Identity, and Closure (HDG SF5 within S5): Establish, deploy, and sustain the corporate integration of HDG policies with other relevant policies to continuously ensure a consistent governance context. Establish the ultimate dark data governance decision-making role within the VSM system-in-focus; thereby providing the logical closure to it. Establish the system's overall data governance direction, policies, values, and purpose and monitor the feedback loop between current (SF3) and future (SF4) data governance systemic functions (in integration with corporate IT governance and corporate governance). This ensures the balance between internal and external perspectives and supports the achievement of present operational and long-term organisational goals.	4.38	88%

Table 6. 6 The mean and consensus% of the participants' feedback on the SFs of Phase 2

Table 6.6 summarizes the feedback on the importance of the six systemic functions (SFs) in Phase 2 of the model. The table presents the ratings provided by various participants for each SF, along with the consensus percentage and mean rating. All SFs achieved more than 60% consensus, indicating strong agreement among participants on their importance in Phase 2. Figure 6.9 shows mean scores and consensus percentages as a graph.

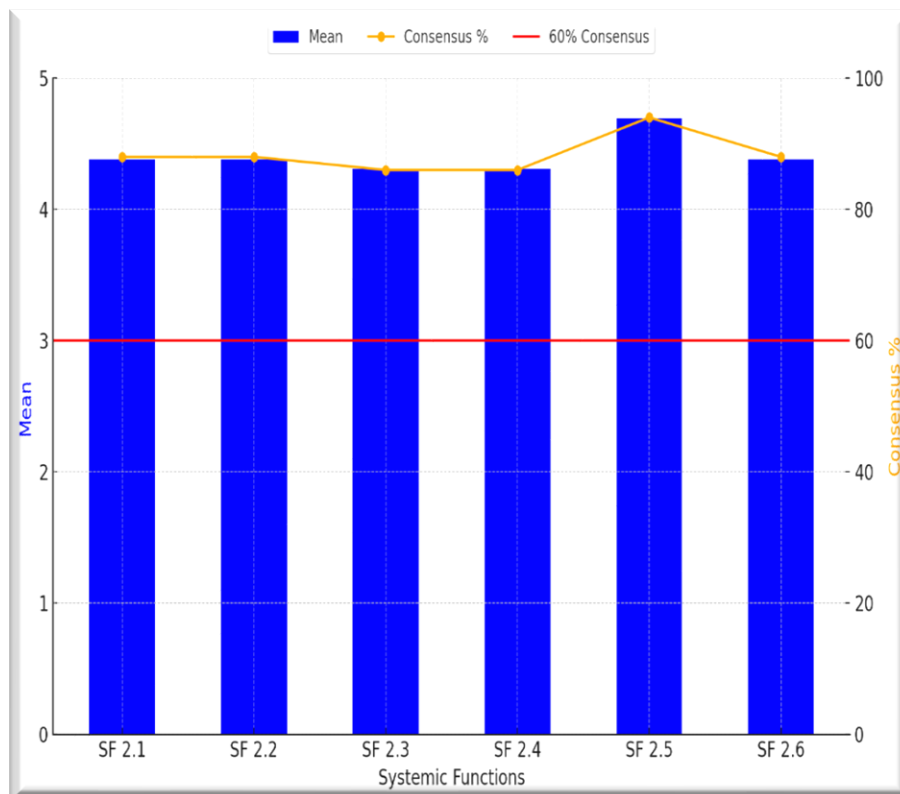


Figure 6. 9 The participants’ feedback on the validation of the SFs of Phase 2

Figure 6.9 is the graph with two y-axes: one for the mean scores and one for the consensus percentages. The mean scores are displayed as bars, while the consensus percentages are shown as a yellow line with a 60% threshold marked by a red line. This visualization allows for a clear comparison of both mean ratings and consensus on the importance across the six SFs.

All systemic functions of HDGM (Phase 2) are highly valued by the participants, with all functions achieving a consensus percentage well above the 60% threshold. The highest-rated function is SF 2.5, highlighting the critical role of research, adaptation, and planning in managing dark data and supporting organisational longevity. Other functions like support to operational units, harmonization, and policy integration also received high ratings, emphasizing their importance in the holistic data governance model. Overall, the results demonstrate a strong endorsement of the systemic functions by the participants.

● Validation Results of Phase 3

This step aims to validate the components of the third phase to make sure that these components are important when identifying the significant requirements for deploying,

assessing, and sustaining the model. Phase 3 includes six systemic functions as components, coded SF 3.1 to SF 3.6. Figure 6.10 shows the participants' feedback on these SFs.

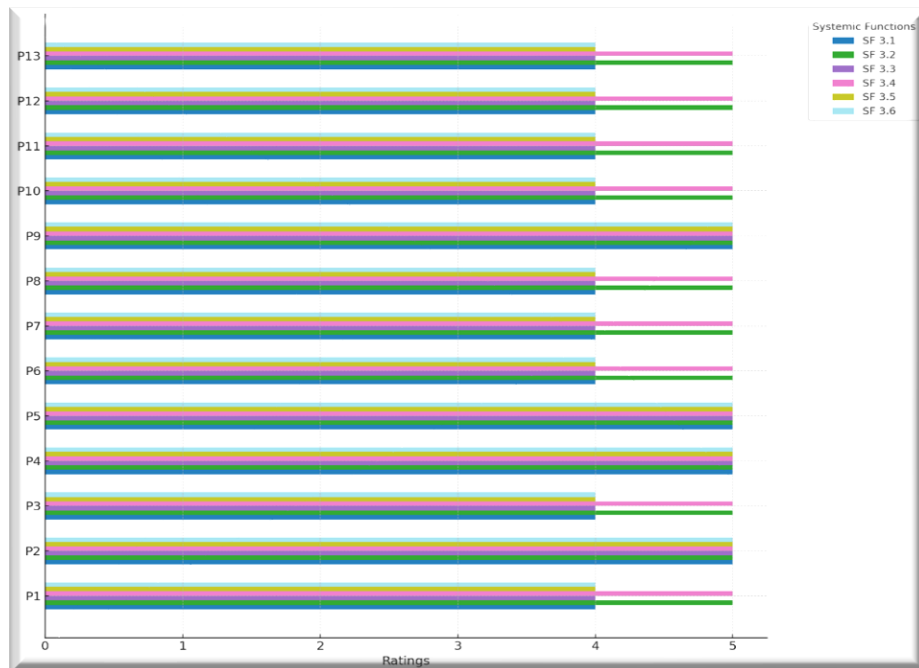


Figure 6. 10 The participants' feedback on the SFs of Phase 3

The graph presents the participants on the y-axis and scores on the x-axis. The bars represent the scores for each systemic function in phase 3. This visualization compares the ratings of each SF by different participants side by side.

Table 6.7 shows the mean and consensus percentage of the participants' feedback.

SF ID	Systemic Function (SF) Description	Mean	Consensus %
SF 3.1	HDG Recursive Systemic Functions (SF6): Identify the level of recursions for the organisation. Recursivity ensures each embedded organisation operates as a viable system itself with appropriate autonomy to self-govern. All data governance systemic functions at different levels of recursions are integrated to counteract dark data and support the achievement of operational and organisational embedded goals.	4.31	86%
SF 3.2	HDG Requisite Variety Systemic Function (SF7): Identify, deploy, and sustain short-term (SF1-Environment) and long-term (SF4-Environment) data governance activities within the system's environment. This is crucial to respond to data governance present	4.97	99%

SF ID	Systemic Function (SF) Description	Mean	Consensus %
	and anticipated organisational data requirements and associated dark data threats to achieve organisational goals.		
SF 3.3	HDG Inter-operational Management Systemic Functions (SF8): Identify, deploy, and sustain key communication channels and key information flows among SF1, SF2, and SF3 within the VSM S1, S2, and S3. This is crucial to balance operational autonomy with data governance control through SF1 data governance support activities within S1 Operations, SF2 data governance coordination and SF3 data governance control systemic functions. This enhances decision-making through self-regulation, cohesion, and synergy to support achieving operational and organisational goals.	4.31	86%
SF 3.4	HDG Adaptability, Learning, and Change Management Systemic Functions (SF9): Identify, deploy, and sustain key communication channels and key information flows among the data governance metasystem functions SF3, SF4, and SF5. This is crucial to provide the organisation with data governance decision-making capabilities, balancing present and future orientations and internal and external perspectives.	4.97	99%
SF 3.5	HDG Communication channels and Algedonic channel Systemic Functions (SF10): Identify, deploy, and sustain key communication channels and key information flows among SF1, SF2, SF3, SF4, and SF5. In crises, the algedonic channel triggers immediate interventions from the metasystem to ensure rapid response to high dark data risks.	4.31	86%
SF 3.6	HDG Common Data Governance Holistic Context (SF11): Identify, deploy, and sustain the common data governance holistic context through the integration of all systemic functions (SF1 to SF5) and their integration within SF1 to SF5 to function cohesively. This ensures the organisation operates as a unified system.	4.31	86%

Table 6. 7 The mean and consensus% of the participants' feedback on the SFs of Phase 3

Table 6.7 summarizes feedback on the importance of the six systemic functions (SFs) in Phase 3 of the model. The table presents the ratings provided by various participants for each SF, along with the consensus percentage and mean rating. All SFs achieved more than 60% consensus, indicating strong agreement among participants on their importance in Phase 3. Figure 6.11 shows mean scores and consensus percentages as a graph Figure 6.11 is the graph with two y-axes: one for the mean scores and one for the consensus percentages. The mean scores are displayed as bars, while the consensus percentages are shown as a yellow line with

a 60% threshold marked by a red line. This visualization allows for a clear comparison of both mean ratings and consensus on the importance across the six SFs.

All systemic functions (SF 3.1 to SF 3.6) have consensus percentages well above the 60% validation agreement threshold. This confirms the robustness and effectiveness of the systemic functions within Phase 3 of HDGM, ensuring they are well supported by consensus.

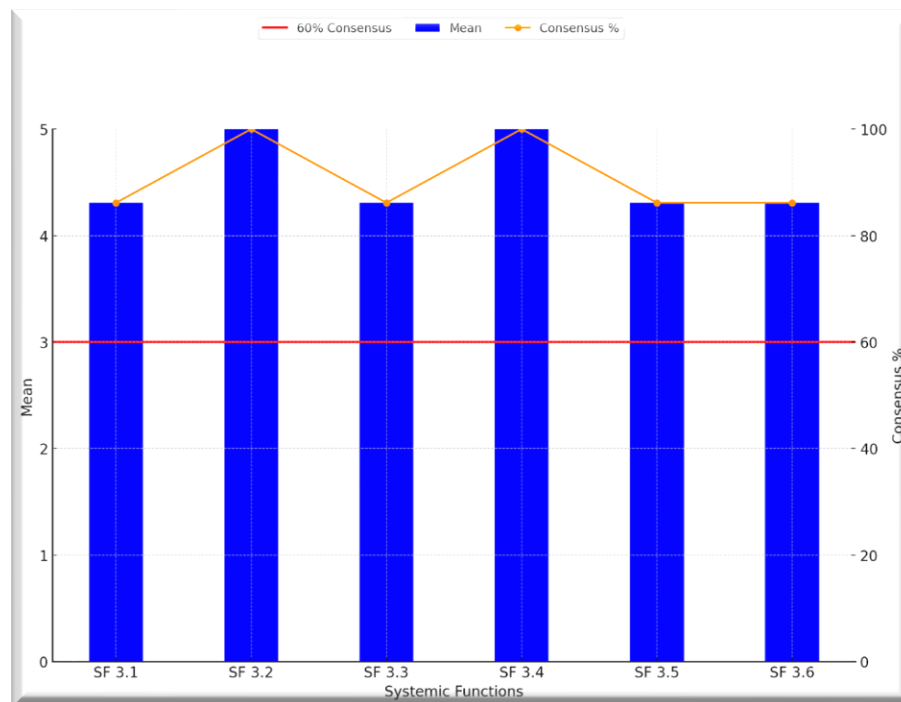


Figure 6. 11 The participants' feedback on the validation of the SFs of Phase 3

6.5.4. Validation Results of the Model's Usability

Validating the usability of the model is critical to ensure it meets the necessary requirements and can be effectively applied within the organisation to counteract dark data and support the achievement of organisational goals. This section aims to evaluate the model's usability in terms of its ease of use, ease of learning, clarity, and coverage of key holistic data governance qualities: scalability, practicality, agility, comprehensiveness, usefulness, efficiency, and innovation Support. This is in addition to the model's added value by supporting the achievement of organisational objectives and by mitigating the risks associated with dark data. This assessment includes seven statements, coded St 3.1 to St 3.7, where participants were asked to indicate their level of agreement or disagreement using a Likert scale from 5 (strongly agree) to 1 (strongly disagree) to rate the overall usability of the model. The consensus of the

participants' feedback on the statements to validate the model usability is illustrated in Figure 6.12, Table 6.8, and Figure 6.13.

Figure 6.12 summarizes the ratings given by each participant regarding the holistic dark data governance model usability for each statement and each participant. Each colour represents a different statement, with participants on the y-axis and scores on the x-axis.

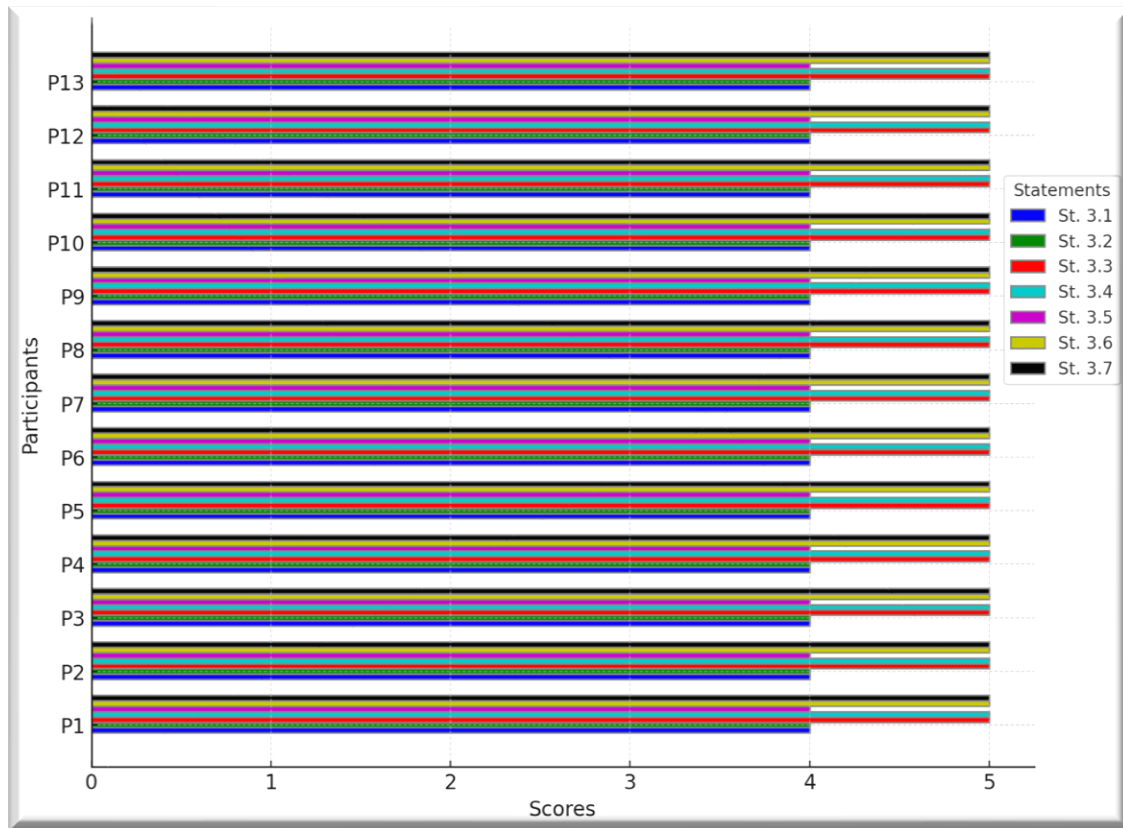


Figure 6. 12 The participants' feedback on the validation statements of the model usability

Table 6.8 summarizes the descriptions for each statement regarding the usability of the holistic dark data governance model along with the percentage of the consensus and the mean rating for the participants' feedback on each statement. The analysis shows strong consensus on the usability of the holistic dark data governance model across all statements.

St. 3.n	Statement	Mean	Consensus %
St. 3.1	The model is easy to use.	4	80%
St. 3.2	The model is easy to learn.	4	80%

St. 3.n	Statement	Mean	Consensus %
St. 3.3	The model is clear and flexible. It can adapt to changing organisational needs and data governance requirements with agility.	5	100%
St. 3.4	The model is scalable, allowing the application to various levels of recursion within the organisation. It is adaptable to different sizes of organisations and data sets.	5	100%
St. 3.5	The model can be practically used and easily integrates with existing systems and technologies within the organisation.	4	80%
St. 3.6	The model provides comprehensive systemic functions that support innovation within the organisation's context.	5	100%
St. 3.7	The model adds value by efficiently counteracting dark data risks and supporting the achievement of organisational goals.	5	100%

Table 6. 8 The consensus and means of the participants' feedback on the statements to validate the model usability

In Figure 6.13, the blue bars represent the mean ratings for each statement, and the yellow line with markers indicates the percentage of consensus for each statement.

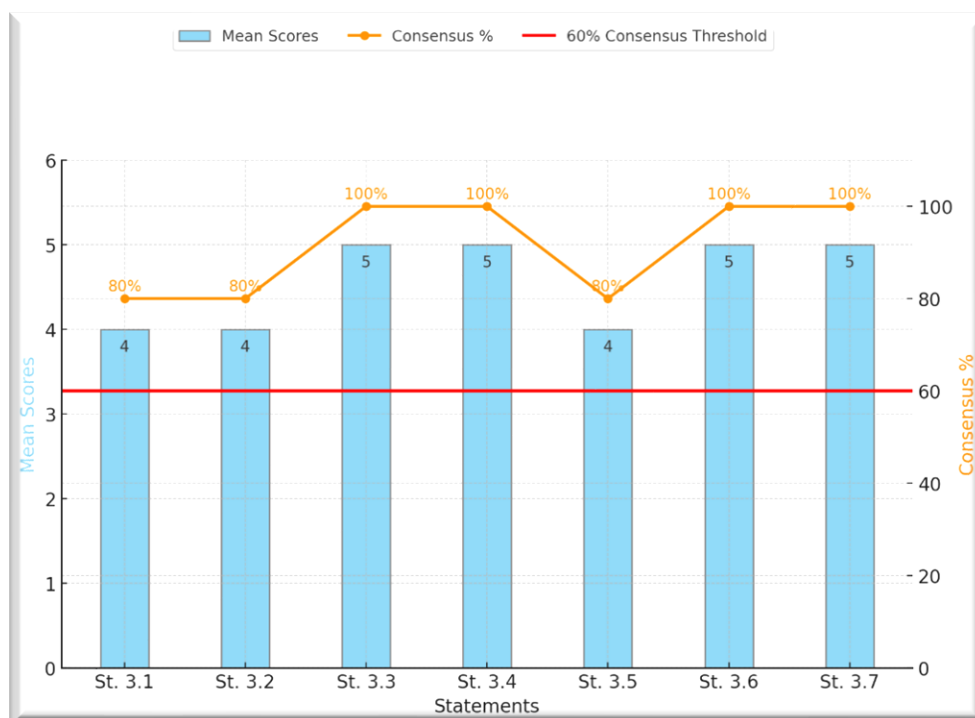


Figure 6. 13 The consensus and means of the participants' feedback on the statements to validate the model usability

The solid red line represents the 60% consensus threshold. This visualization effectively highlights the consensus threshold along with the ratings and consensus levels for each statement.

All the usability statements for HDGM have consensus percentages well above the 60% validation agreement threshold. This indicates strong agreement among participants regarding the model's ease of use, learnability, flexibility, scalability, practical integration, support for innovation, and value addition. The high mean scores further reinforce the positive perception and validation of the HDGM effectiveness and usability by all participants.

6.5.5. Findings and Discussion

Given the results of the analysis above, the Likert scale frequency was used to measure the participants' feedback. The Likert scale answers for each statement, along with the mean and percentage of consensus, were considered in the data analysis. Table 6.3 summarizes the data as assessed by the participants, validating the model design in supporting the aims and objectives of the dark data governance holistic model. The consensus percentage results (> 60%) indicate that most participants agree with all the statements as shown in Figure 6.14.

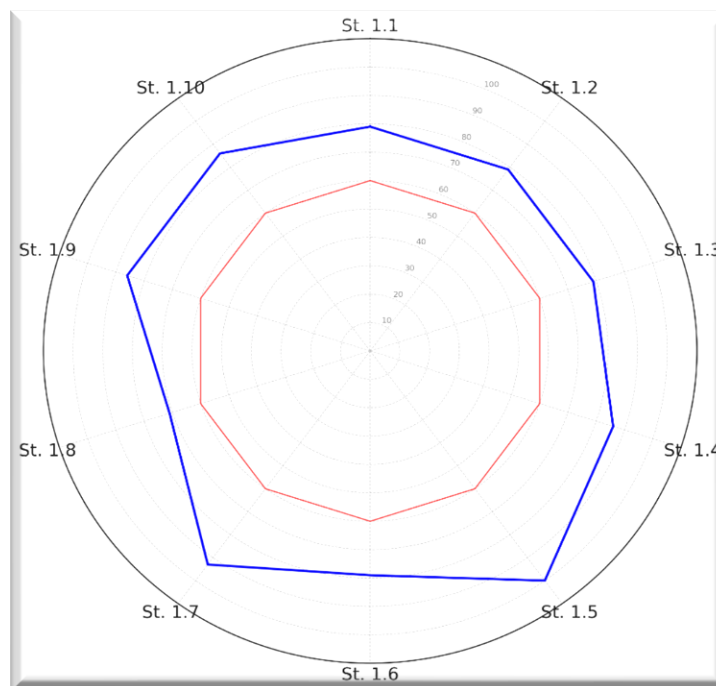


Figure 6. 14 The consensus percentage results of the model design

Regarding the validation of the model's phases, the results demonstrate strong participant agreement that all the given systemic functions are crucial for counteracting dark data risks and supporting organisational goals. Furthermore, the participants validated the importance of each

phase's proposed systemic functions. The consensus percentages indicate general agreement with all the given systemic functions as shown in Figure 6.15.

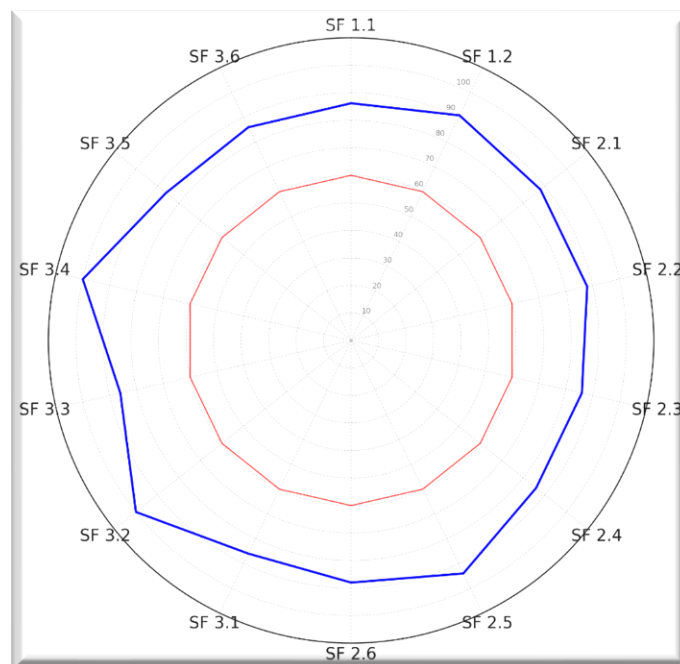


Figure 6. 15 The consensus percentage results of the model phases-SFs

Additionally, the participants validated the model's usability with strong agreement, with consensus percentages well above the 60% validation agreement threshold. This high level of agreement emphasizes the model's effectiveness and usability in addressing dark data governance challenges and achieving organisational objectives as shown in Figure 6.16.

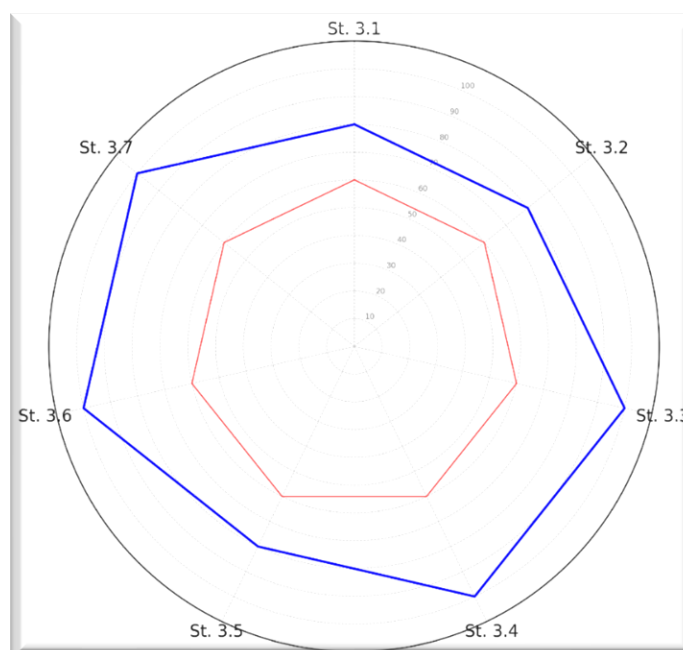


Figure 6. 16 The consensus percentage results of the model usability

6.5.6. Overall Validation of the Proposed Model and Suggestions for Model Improvements

The validation process aimed to assess the applicability of the proposed model within a university context by modifying or expanding on the systemic functions presented in Figure 4.10 in Chapter 4. Utilizing the Delphi method's structured and systematic approach allowed for the iterative refinement and enhancement of ideas, leading to a more comprehensive and validated model for holistic dark data governance. To ensure the reliability and validity of the qualitative analysis conducted using the Delphi technique, several measures were implemented (detailed in Chapter 2). By incorporating these measures, the Delphi technique used in this study was designed to produce reliable and valid qualitative data, enhancing the robustness of the research findings. This approach enhanced the credibility of the outcomes, to effectively refine the proposed model.

Accordingly, the systemic functions of each phase identified for the proposed model in Chapter 4 (Figure 4.10) were validated through participants' feedback on the closed questions, with the results presented in Table 6.9. Also, improvements were suggested by the experts, achieving a consensus above 60%, based on participants' feedback from the open questions. These results are detailed in Table 6.10.

Phase ID	Systemic Function	Consensus %	Confirmation of the Systemic Function
Phase 1	SF 1.1	86%	Fully Confirmed
	SF 1.2	90%	Fully Confirmed
Phase 2	SF 2.1	88%	Fully Confirmed
	SF 2.2	88%	Fully Confirmed
	SF 2.3	86%	Fully Confirmed
	SF 2.4	86%	Fully Confirmed
	SF 2.5	94%	Fully Confirmed
	SF 2.6	88%	Fully Confirmed
Phase 3	SF 3.1	86%	Fully Confirmed
	SF 3.2	100%	Fully Confirmed

Phase ID	Systemic Function	Consensus %	Confirmation of the Systemic Function
	SF 3.3	86%	Fully Confirmed
	SF 3.4	100%	Fully Confirmed
	SF 3.5	86%	Fully Confirmed
	SF 3.6	86%	Fully Confirmed

Table 6. 9 The results of the investigation by the participants

Regarding qualitative feedback, the validation of the model included open-ended statements, allowing participants to express additional comments and recommendations for updating and improving the proposed model. The qualitative feedback revealed several recommendations for enhancing the model, which included the following amendments as illustrated in Table 6.10:

Phase ID	Systemic Function	Suggested Improvements
Phase 1	SF 1.1	Include a definition of the operational units within the organisational VSM system in focus. This is essential for establishing a clear business scope and setting the boundaries of the organisation.
	SF 1.2	Explicitly include the integration of dark data HDG with IT governance and other relevant governance domains to ensure a systemic holistic context.
Phase 2	SF 2.1	Explicitly include the integration of dark data HGD SF1 with IT governance and other relevant governance domains to ensure a systemic holistic context.
	SF 2.2	Explicitly include the integration of dark data HDG SF2 with IT governance and other relevant governance domains to ensure a systemic holistic context.
	SF 2.3	Explicitly include the integration of dark data HDG SF3 with IT governance and other relevant governance domains to ensure a systemic holistic context.

Phase ID	Systemic Function	Suggested Improvements
	SF 2.4	Explicitly Ensure that integration of dark data HDG SF3* with IT governance and other relevant governance are considered within a systemic holistic context
	SF 2.5	Explicitly include the integration of dark data HDG SF4 with IT governance and other relevant governance domains to ensure a systemic holistic context.
	SF 2.6	Explicitly include the integration of dark data HDG SF5 with IT governance policies and other relevant governance policies to ensure a consistent systemic holistic context.
Phase 3	SF 3.1	Explicitly include that the model of data governance that provides a systemic holistic corporate context at the organisational level is taking into consideration the integration with IT governance and other relevant governance domains
	SF 3.2	Explicitly include the integration of dark data HDG SF7 with IT governance and other relevant governance domains to ensure a systemic holistic context.
	SF 3.3	Explicitly include the integration of dark data HDG SF8 with IT governance and other relevant governance domains to ensure a systemic holistic context.
	SF 3.4	Explicitly include the integration of dark data HDG SF9 with IT governance and other relevant governance domains to ensure a systemic holistic context.
	SF 3.5	Explicitly include the integration of dark data HDG SF10 with IT governance and other relevant governance domains to ensure a systemic holistic context.
	SF 3.6	Explicitly include the integration of dark data HDG SF11 with IT governance and other relevant governance domains to ensure a systemic holistic context.

Table 6. 10 The improvements suggested by the participants

6.5.7. Model Refinement

As discussed above, the qualitative feedback indicated that participants suggested improvements to the systemic functions of the proposed model. Therefore, these suggestions have been considered and incorporated into this research to enhance the proposed model. The recommendations have been addressed, and the proposed model has been amended accordingly, as illustrated in Table 6.11 and Figure 6.17.

Systemic Phase 1: Identify the Organisational VSM System-in-focus and Contextualize, and Sustain the Holistic Dark Data Governance Sub-System (HDGM) within the VSM Context to counteract dark data risks and support the achievement of the organisational goals	
SF. 1.n	Systemic Function
SF 1.1	Identify the organisational VSM system-in-focus (Organisational level) with its purpose, goals, stakeholders, and boundaries of the organisation within its environment. Define Operational units within the organisational VSM system in focus. This is essential for establishing a clear business scope and setting the boundaries of the organisation. Define dark data governance purpose. Dark Data governance purpose for this study is to counteract dark data risks and create business value to support organisational viability and goal achievement.
SF 1.2	Contextualize, deploy and sustain the scope to support the goals of the holistic data governance model (HDGM) as a subsystem within the organisational VSM system-in-focus) in integration with IT governance and other relevant governance domains. The goal is mainly to counteract dark data risks and support organisational viability and goal achievement within a systemic holistic context.
Systemic Phase 2: Identify, Deploy, and Sustain the Holistic Dark Data Governance (HDG) Systemic Functions (SFs) within the Organisational VSM system-in-focus (Organisational Level) to counteract dark data risks and support the achievement of the organisational goals	
SF. 2.n	Systemic Function
SF 2.1	HDG SF1 Support to Operational Units (HDG SF1 within VSM S1): Identify, deploy, and sustain HDG policies, guidelines, and procedures, in integration with IT

	governance and other relevant governance domains, to provide core activities with necessary data and counteract dark data risks within a systemic holistic context. HDG SF1 supports organisational viability and the achievement of operational goals.
SF 2.2	HDG Harmonisation (HDG SF2 within VSM S2): define, deploy and sustain compliance with corporate dark data governance systemic functions in integration with IT governance and other relevant governance domains (e.g. corporate policies, guidelines, standards, rules, and protocols) to prevent recurrent dark data governance conflicts and misalignment among primary units within S1 within a systemic holistic context. Deploy identified corrective actions and continuously improve as appropriate to support corporate harmonization. HDG SF2 supports organisational viability and the achievement of operational goals.
SF 2.3	HDG Cohesion & Autonomy (HDG SF3 within VSM S3): define, develop, and sustain SF3 corporate dark data governance systemic functions in integration with IT governance and other relevant governance domains within a systemic holistic context: HDG Corporate policies, HDG performance measurements, HDG compliance requirements, HDG resource requirements (e.g. Technology, Financials, competencies) requirements, and allocation of HDG resources to SF1. Corporate policies are developed for key data governance domains: Data Architecture, Data Quality, Metadata, Data Security, Reference & Master Data, Data Warehousing/Business Intelligence/Artificial Intelligence, Data Modelling & Design, Document & Content Management, Data Storage & Infrastructure/Operation, Data Integration & Interoperability. HDG SF3 supports the balance between self-regulation (Autonomy) for each operational unit in S1 and their synergies (Cohesion) amongst them for improved organisational performance and achievement of operational and organisational goals.
SF 2.4	HDG Audit and Compliance (HDG SF3* within S3*): Define, conduct and sustain data governance auditing and compliance functions to gather information about data requirements and dark data challenges from S1 units. Ensure that integration with IT governance and other relevant governance domains are considered within a systemic holistic context. Accordingly, results and improvements are shared through key communication channels among SF3, SF3*, and SF1. This is to support the achievement of organisational goals.
SF 2.5	HDG Intelligence /Adaptation (HDG SF4 within S4): Conduct research, development, and corporate planning to make sense of the environmental changes such as constraints and opportunities related to data needed by the organisation and

	potentially encountering dark data that could threaten organisational viability. This is conducted in integration with IT governance and other relevant governance domains to ensure a systemic holistic context. Deploy and sustain the holistic data governance strategy and long-term orientated tasks to support and improve the adaptability and the achievement of the organisation's long-term goals
SF 2.6	HDG Policy, Identity, and Closure (HDG SF5 within S5): Establish, deploy, and sustain the corporate integration of dark data HDG policies with other relevant governance policies (e.g. IT governance and other relevant governance domains) to continuously ensure a consistent systemic holistic context. Establish the ultimate dark data governance decision-making role within the VSM system-in-focus; thereby providing the logical closure to it. Establish the system's overall data governance direction, policies, values, and purpose and monitor the feedback loop between current (SF3) and future (SF4) data governance systemic functions (in integration with corporate IT governance and corporate governance). This ensures the balance between internal and external perspectives and supports the achievement of present operational and long-term organisational goals
Systemic Phase 3: Identify, Deploy, and Sustain the Key Interactions (Variety loops /Feedback loops) among the Holistic Dark Data Governance Systemic Functions (HDG SFs) within the Organisational VSM system-in-focus to counteract dark data risks and support the achievement of the organisational goals	
SF. 3.n	Systemic Function
SF 3.1	HDG Recursive Systemic Functions (SF6): Identify the level of recursions for the organisation. Recursivity ensures that each embedded organisation operates as a viable system itself (with appropriate autonomy to self-govern). All data governance systemic functions at different levels of recursions are integrated to counteract dark data and support the achievement of operational and organisational embedded goals. The VSM is fractal in nature, meaning that each viable system, at any given level of recursion, can be modelled using exactly the same syntax and this is applied to SF6 Systemic functions at each level of recursion. To develop and sustain a model of dark data governance that provides a systemic holistic corporate context in integration with IT governance and other relevant governance domains, this research adopts the organisation as the specific unit of analysis. Accordingly, the model can be applied at any other level of recursion since it has the same structural context

SF 3.2	HDG Requisite Variety Systemic Function (SF7): Identify, deploy, and sustain short-term (SF1-Environment) and long-term (SF4-Environment) data governance activities (key communication channels and key information flows) within the system's environment. This is identified in integration with IT governance and other relevant governance domains to ensure a systemic holistic context. This is crucial to respond to data governance present (SF1) and anticipated organisational data requirements (SF4) and the associated dark data threats to achieve organisational goals. HDG SF7 must possess adequate internal variety to effectively govern the data assets and counteract dark data risks in response to external digital disruptions and new data governance regulations, thereby establishing the requisite variety needed. Detecting and responding to dark data threats and opportunities is crucial to support the organisation's viability. This enables the organisation to remain agile and responsive to environmental changes.
SF 3.3	HDG Inter-operational Management Systemic Functions (SF8): Identify, deploy, and sustain key interactions, communication channels, and key information flows among the dark data HDG systemic functions: SF1, SF2, and SF3 (within the VSM S1, S2, and S3 within key interactions among VSM S1, S2, and S3). This is identified in integration with IT governance and other relevant governance domains to ensure a systemic holistic context. This is crucial to balance operational autonomy with data governance control through SF1 data governance support activities within S1 Operations, SF2 data governance coordination, and SF3 data governance control systemic functions. This enhances decision-making through self-regulation, cohesion, and synergy to support achieving operational and organisational goals
SF 3.4	HDG Adaptability, Learning, and Change Management Systemic Functions (SF9): Identify, deploy, and sustain key communication channels and key information flows among the data governance metasystem functions SF3, SF4, and SF5 (within the S3, S4, and S5 corporate metasystem). This is identified in integration with IT governance and other relevant governance domains to ensure a systemic holistic context. This is crucial to provide the organisation with data governance decision-making capabilities. It balances present and future orientations and internal and external perspectives to maintain homeostasis regarding data governance and dark data handling. Key communication channels and key information flows facilitate coordination, innovation, adaptability, learning, and change management in data governance and dark data handling activities. This supports the achievement of operational and organisational goals.
SF 3.5	HDG Communication channels and Algedonic channel Systemic Functions (SF10): Identify, deploy, and sustain key communication channels and key

	information flows among SF1, SF2, SF3, SF4, and SF5. This is identified in integration with IT governance and other relevant governance domains to ensure a systemic holistic context. This is crucial to counteract dark data at all levels and for all types of dark data. However, in crises, the algedonic channel (SF1 to SF5 directly) triggers immediate interventions outside the normal regulatory channels from the metasytem. This ensures a rapid response to situations with high dark data risks, such as security breaches, thereby supporting the achievement of operational and organisational goals.
SF 3.6	HDG Common Data Governance Holistic Context (SF11): Identify, deploy, and sustain the common data governance holistic context through the integration (key communication channels and information flows) of all systemic functions (SF1 to SF5) and integration within SF1 to SF5 that must function cohesively. This is identified in integration with IT governance and other relevant governance domains to ensure a systemic holistic context. This is crucial to ensure the organisation operates as a unified system, rather than isolated parts. SF11 facilitates the integration among all data governance systems through transduction, which involves having a shared language (metadata, e.g. dark data types, data types) across all systems related to data and dark data types. Such shared understanding improves communication between business and data stakeholders, creating common data governance knowledge and reducing potential dark data risks across the organisation. This also enhances organisational data governance culture, impacting business operations and supporting the achievement of operational and organisational goals.

Table 6. 11 Amended model (HDGM) after participants' feedback

This study has examined and presented a methodology to deploy, assess, and sustain the Holistic Dark Data Governance Model (HDGM), which aims to help organisations, particularly universities, implement an effective dark data governance system. The study is novel in identifying key systemic functions that constitute the model of dark data governance. The proposed and confirmed dark data governance systemic functions within the Viable System Model (VSM) organisational context are presented in the confirmed HDGM (Figure 6.17).

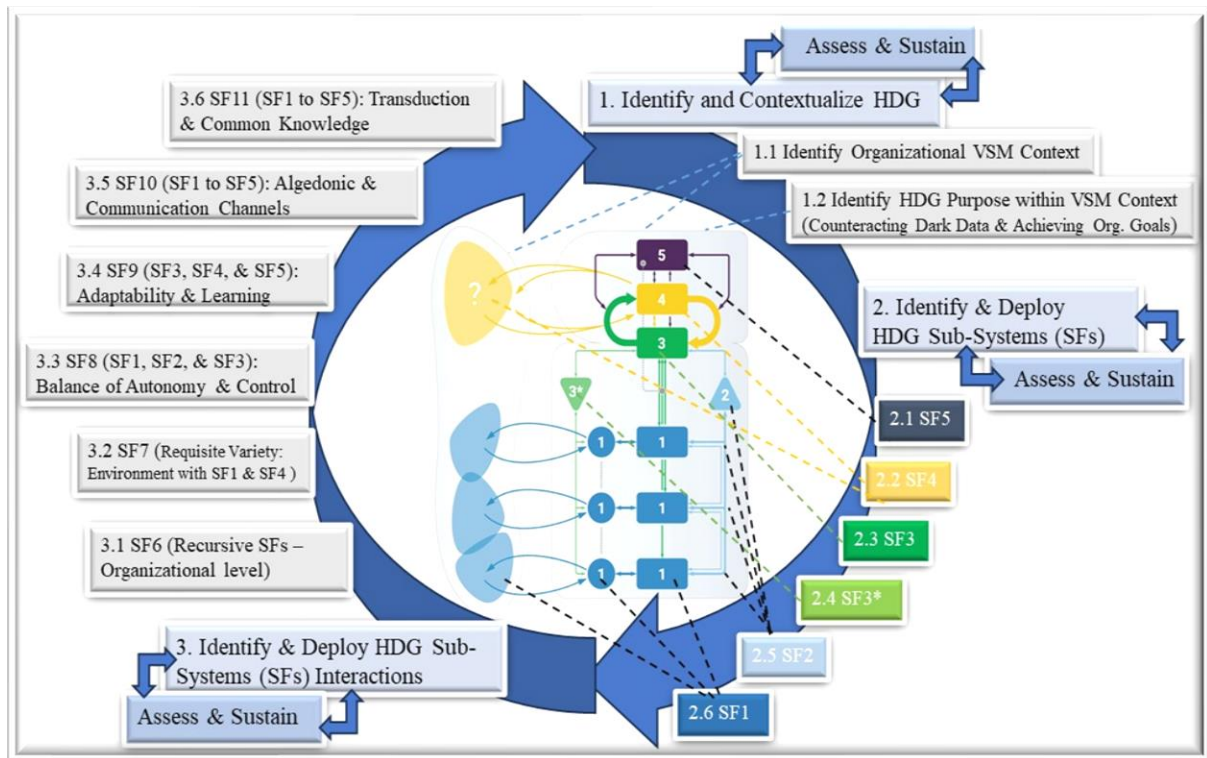


Figure 6. 17 Confirmed Model (HDGM) after Participants' Feedback

6.6. Chapter Summary

The validation of the Holistic Dark Data Governance Model (HDGM) references a robust theoretical foundation and was conducted through a systematic and iterative Delphi method involving a panel of 13 experts from a key university in Texas, USA. The validation process addressed key research questions on dark data governance components, the impact of holistic data governance, and the emphasis on key data governance concepts. Feedback was collected in three rounds, allowing for refinement and consensus-building. The results demonstrated strong agreement on the model's design, systemic phases, and functions, with recommendations for improvements incorporated into the final version. This rigorous process ensured the model's reliability and validity, enhancing its applicability for managing dark data within organisations. The final HDGM integrates feedback and suggestions to create a comprehensive and validated model for holistic data governance, ensuring it supports organisational goals and mitigates dark data risks effectively. The following chapter presents a viability maturity approach for the Holistic Dark Data Governance Model, along with a corresponding performance assessment matrix. These frameworks are designed to evaluate the viability maturity of dark data governance within organisations, thereby ensuring that the model addresses current requirements while also supporting ongoing viability and continuous improvement.

Chapter 7: Evaluation of the Dark Data Governance Maturity Model and Maturity Assessment Matrix

7.1. Introduction

The maturity model presented in Chapter Five aims to guide organisations in assessing their current holistic dark data governance capabilities and formulating new objectives based on emerging requirements and environmental shifts, in order to support the achievement of organisational goals. The maturity model was developed based on the proposed holistic model presented in Chapter Four, in order to define the specific maturity model dimensions and corresponding maturity levels that organisations can use to assess their current holistic dark data governance capabilities and identify areas for improvement. Furthermore, a dark data governance assessment matrix was proposed as a tool to assist with evaluating the organisation's dark data governance holistic context during the assessment process. The dark data governance assessment matrix is intended to identify the strengths and constraints of the organisation's dark data governance practices, and to provide recommendations for improving the overall holistic dark data governance process within the organisation to facilitate the achievement of organisational goals. Having developed the holistic dark data governance maturity model and assessment matrix, it is crucial to test and evaluate their validity before they can be more widely disseminated and implemented across organisations. This evaluation process is essential to ensure the practical applicability and effectiveness of the proposed models, and to identify any areas that may require further refinement or enhancement. By thoroughly evaluating the maturity model and assessment matrix, the research can contribute to the establishment of a robust and reliable framework for assessing and improving dark data governance capabilities within organisations. The assessment of the model's accuracy and applicability in representing reality will be informed by expert evaluation. Prior studies have employed a variety of methods to validate and evaluate frameworks and models, including surveys, case studies, questionnaires, focus groups, interviews, and workshops (Kennedy, W., 2005); (Oberkampff, L. W. and Trucano, T., 2008); (Martínez, F. A. and Largo, L. F., 2009). In this research, the proposed model was evaluated through a Delphi Study for the case of a key university in Texas, USA. The experts involved in this evaluation hold diverse roles as illustrated in Table 7.1. The expert recommendations were thoroughly considered and incorporated in order to adjust and refine the proposed maturity model and assessment matrix. The insights gained from the evaluation procedures were carefully analysed, and the necessary modifications were made to ensure the practical applicability and effectiveness of the models.

The findings from each of the evaluation activities, which employed the Delphi approach for the key university in Texas, USA (University X), are examined in depth below.

7.2. Design of the Validation Approach

The purpose of this thesis was to assist key universities in Texas, USA, with implementing an effective holistic model for governing dark data. Consequently, the holistic dark data governance maturity model and its corresponding assessment matrix were developed to aid in evaluating the organisation's dark data governance practices, and to offer recommendations for enhancing the overall holistic dark data governance process within the organisation, thereby facilitating the achievement of institutional objectives. Therefore, this chapter focuses on evaluating the maturity model and its assessment matrix. The Delphi method was employed to evaluate the maturity model due to its suitability for eliciting expert opinions and achieving consensus on complex issues (Sargent, 2013). This technique involves a panel of experts participating in iterative rounds of questions, with feedback provided to refine responses as necessary. The advantages of the Delphi method for this study include participant anonymity, controlled feedback, and aggregation of judgments into a consensus (Omar and almaghthawi, 2020). Utilizing this method allowed for a systematic and iterative approach to refining the maturity model, integrating expert insights, and reducing biases. The research involved selecting a panel of thirteen experts in governance and management, designing questionnaires, conducting the required rounds of data collection, and achieving a consensus of 60% or higher. This approach facilitated a comprehensive examination of holistic data governance, ultimately leading to a validated maturity model and its assessment matrix (Gale et al., 2013).

7.3. Panel of Experts Validation Scope

The evaluation by the panel of experts focused on the following aspects, which are elaborated in the subsequent sections:

- Identifying the appropriate assessment criteria to be used in evaluating the maturity model and its assessment matrix
- Outlining the evaluation approach, including the panel's feedback and an analysis of the evaluation results
- Updating the proposed dark data governance model based on the participants' feedback, where a consensus of at least 60% was achieved

7.4. Assessment Criteria

Academic literature has explored the development of evaluation and validation criteria, also referred to as success criteria or quality aspects, for research models and frameworks. Consequently, this section investigates approaches to selecting suitable criteria for evaluating the proposed maturity model and its assessment matrix. Beecham et al. proposed a set of seven criteria to evaluate the strengths and weaknesses of the R-CMM (Requirements Capability Maturity Model) maturity model (Beecham et al., 2005). These criteria included evaluating the model's adherence to Capability Maturity Model characteristics, defined scope, consistency, understandability, ease of use, customizability, and verifiability. Boehm and Valerdi (Boehm and Valerdi, 2008) proposed a set of criteria to evaluate the practical utility of software cost estimation models. These criteria include definition, fidelity, objectivity, constructiveness, detail, stability, scope, ease of use, prospectiveness, and parsimony, which were presented in the form of evaluative questions. Niazi and colleagues developed a Requirements Engineering (RE) maturity measurement framework to assess the strengths and weaknesses of RE practices within the model, utilizing two key success criteria: user satisfaction and ease of use (Niazi, Cox and Verner, 2007). These criteria were adapted from the widely-recognized Technology Acceptance Model proposed by Davis, which has been extensively used and validated in various information systems research studies to evaluate user acceptance of new technologies (Davis, 1989). Solomen et al. (Solemon, 2013) proposed a set of five criteria to evaluate the effectiveness of requirements engineering process improvement models, including completeness, consistency, practicality, usefulness, and verifiability. These criteria can be adapted and applied to assess the holistic dark data governance maturity model and its corresponding assessment matrix, in order to enhance their comprehensiveness and practical applicability.

After analysing all the proposed criteria in the literature, the following five criteria were selected for evaluating the proposed maturity model, each with associated sub-criteria:

1. **Completeness:** Evaluating the extent to which the maturity model comprehensively covers all relevant aspects of holistic dark data governance.
2. **Consistency:** Assessing the coherence and logical flow of the maturity model's structure, dimensions, and level descriptions.
3. **Practicality:** Determining the feasibility and applicability of the maturity model in real-world organisational settings.

4. Usefulness: Evaluating the model's ability to provide meaningful insights and recommendations for improving holistic dark data governance practices.
5. Verifiability: Assessing the model's ability to be validated and its results replicated through empirical evidence.

Similarly, the following six criteria were selected for evaluating the proposed assessment matrix:

1. Completeness: Evaluating the extent to which the assessment matrix covers all relevant aspects of holistic dark data governance.
2. Consistency: Assessing the coherence and logical flow of the assessment matrix's structure, dimensions, and level descriptions.
3. Practicality: Determining the feasibility and applicability of the assessment matrix in real-world organisational settings.
4. Usefulness: Evaluating the matrix's ability to provide meaningful insights and recommendations for improving holistic dark data governance practices.
5. Verifiability: Assessing the matrix's ability to be validated and its results replicated through empirical evidence.
6. Strengths and Weaknesses: Identifying the strengths and weaknesses of the assessment matrix to guide further improvements.

The proposed criteria will be evaluated using a combination of quantitative and qualitative research methods. The quantitative approach will involve the use of a Likert-scale to assess the frequency of the participants' responses for each criterion. This will provide a numerical measure of the experts' perceptions of the completeness, consistency, practicality, usefulness, verifiability and strengths, weaknesses of the maturity model and assessment matrix. Additionally, a qualitative research method will be employed, which will involve the collection and analysis of the participants' suggestions and feedback. This will allow for a more in-depth understanding and potential improvements to the proposed model and matrix, based on the expert panel's expertise and insights.

7.5. Evaluation of Holistic Data Governance Maturity Model and Assessment Matrix

The feedback from the evaluation was gathered using a systematic Delphi approach to data collection and analysis. This method facilitated refinement, idea development, and consensus-building among the experts, as described in Section 7.2. Awareness and clarification sessions conducted throughout the process addressed questions in (Appendix O) and ensured

participants fully understood the process. These sessions also facilitated the signing of relevant ethical forms (Appendix B), ensuring compliance and transparency.

The following steps were carried out:

- Awareness and training sessions were conducted on the background of the research, including the problem, aim, objectives, and desired outcomes.
- Awareness and training sessions were conducted on the proposed maturity model and assessment matrix, along with an explanation of their development and implementation. This ensured a comprehensive understanding and provided necessary clarification on the maturity model throughout the data collection process. These sessions also helped address any questions during the Delphi rounds to ensure clarity.
- A questionnaire was distributed (Questions in 3 rounds – Appendix O) to evaluate the proposed maturity model and assessment matrix based on the selected assessment criteria:
 - Completeness was evaluated using closed questions with a five-point Likert scale to obtain participant feedback.
 - Consistency was evaluated using closed questions with a five-point Likert scale to obtain participant feedback.
 - Practicality was evaluated using closed questions with a five-point Likert scale to obtain participant feedback.
 - Usefulness was evaluated using closed questions with a five-point Likert scale to obtain participant feedback.
 - Verifiability was evaluated using closed questions with a five-point Likert scale to obtain participant feedback.
 - The Strengths and Weaknesses of the assessment matrix were evaluated using closed questions with a five-point Likert scale to obtain participant feedback in the second and third rounds.
 - Suggestions from participants to improve the holistic dark data governance maturity model and assessment matrix were obtained using open-ended questions.
- Content analysis of the collected data was performed, ensuring at least a 60% consensus among participants. Based on the recommendations and evaluation results from the expert panel, improvements, and updates were defined for the proposed models in the different rounds, ensuring the changes reflect an expert consensus of 60% or above.
- The proposed HDG maturity model and the assessment matrix were updated to produce the final version of the model and the matrix.

7.6. Deliverables

The key deliverables from the expert panel evaluation are the unique and verifiable outcomes that enable enhancements and improvements to the holistic dark data governance maturity model's levels, dimensions, and level names, as well as refinements to the assessment matrix content. These deliverables, driven by the experts' recommendations and evaluation findings, facilitated the updates and refinements to the proposed HDG maturity model and assessment matrix. The expert evaluation and collaborative refinement process ensured that the final versions of the maturity model and assessment matrix incorporated comprehensive, coherent, feasible, meaningful, and empirically verifiable enhancements to enable organisations to assess and advance their holistic dark data governance capabilities in support of their overall organisational goals.

7.7. Participants' Profiles

The panel of experts included thirteen participants (coded P1 to P13) from a key university (University X with size > 5,000) in Texas, USA. The participants were selected based on their shared educational background and recent experience in developing self-assessment models and matrices, as well as their extensive knowledge and proficiency in the domains of data governance, Information Technology governance, and general governance principles. The data collection process aimed to gather feedback from various departments and management levels simultaneously. This cross-functional and multi-level approach ensured a comprehensive understanding of diverse perspectives and experiences, which enhanced the reliability, depth, and richness of the feedback obtained. By capturing input from different functional areas and organisational hierarchies, the researchers were able to gain a more holistic and well-rounded understanding of the proposed maturity model and assessment matrix, leading to more meaningful and impactful insights for further refinement. Table 7.1 presents the demographic characteristics of the participants. The participants represent a diverse array of roles, demonstrating varying levels of expertise in data/IT governance, self-assessment modelling, and general governance practices. The group includes senior-level positions such as President, Vice President of Technology & Information, Chief Compliance Officer, and Chief Audit Executive, as well as more specialized roles like Data Governance Manager, IT Manager, Data Governance Senior Analyst, and Data Governance Coordinator. The academic perspectives are provided by Professors and a Researcher, while a Director of Learning & Development and a Graduate Student contribute a broader organisational viewpoint. The participants' experience in their current roles ranges from 4 to 13 years, and their data/IT governance expertise spans 3

to 11 years, demonstrating a substantial depth of knowledge in specific governance domains. Additionally, the participants have experience in self-assessment model and matrix utilization ranging from 3 to 9 years, and their general governance experience varies from 2 to 10 years, reflecting a diverse set of expertise levels. The participants' varied roles, from senior leadership positions to specialized governance roles and academic perspectives, as well as their differing periods of employment in their current roles and governance-related experience, demonstrate a comprehensive understanding of the university's governance practices and context.

Participant Code	Role	Experience in Current Job (years)	Data/IT Governance Experience (years)	Self-assessment model and matrix Experience (Years)	General Governance Experience (Years)
P1	President	11	5	3	10
P2	Vice President (Technology & Information)	10	7	4	10
P3	Chief Compliance Officer	9	5	3	7
P4	Data Governance Manager	13	11	7	10
P5	IT Manager	10	7	5	10
P6	Chief Audit Executive	12	4	8	6
P7	Data Governance Senior Analyst	10	9	9	6
P8	Director of Learning & Development	7	4	3	5
P9	Professor – Graduate School	8	4	3	5
P10	Researcher	9	5	4	3
P11	Student – Graduate School	4	3	3	2

P12	Data Governance Coordinator	9	7	6	5
P13	Professor Undergraduate School	10	5	3	4

Table 7. 1 The demographic characteristics of the participants

7.8. HDG Maturity Model Evaluation

This study selected five main criteria to evaluate the proposed holistic dark data governance maturity model: completeness, consistency, practicality, usefulness, and verifiability. Each of these criteria contained several sub-criteria. The study presents the assessment results based on both quantitative and qualitative feedback obtained from the expert panel. A Likert scale was employed, where respondents specified their level of agreement or disagreement on a symmetric agree-disagree scale for a series of statements regarding the maturity model. Figure 7.1 illustrates the overall evaluation process undertaken in this study for examining the holistic dark data governance maturity model

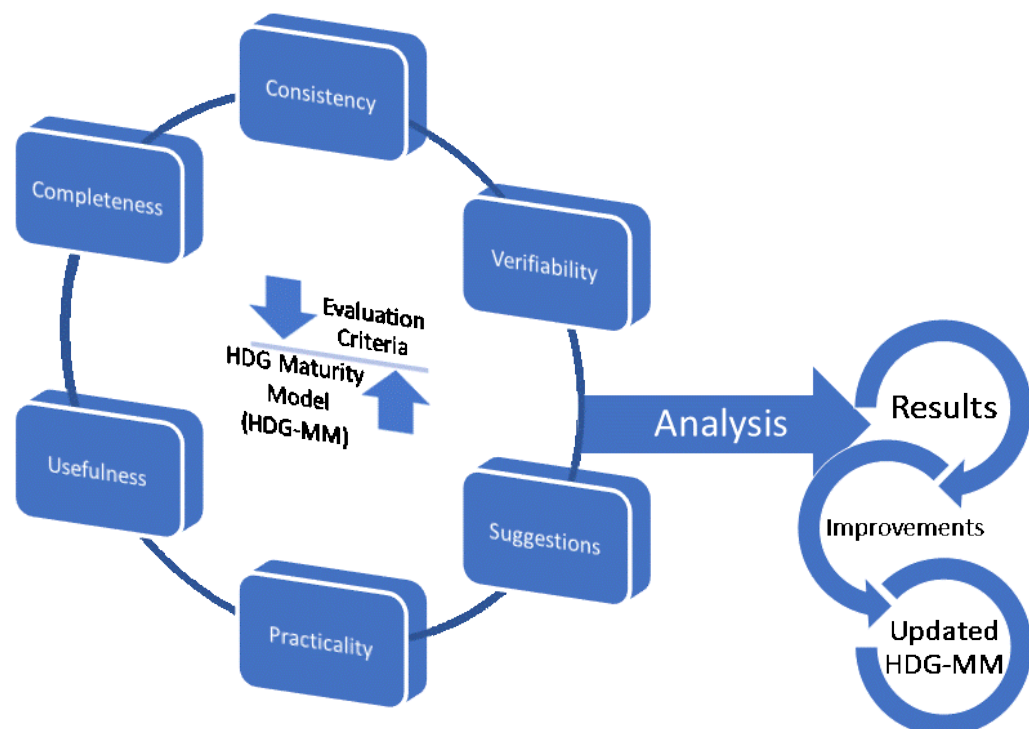


Figure 7. 1 The holistic dark data governance maturity model evaluation process

The results for each criterion are presented below:

7.8.1. Completeness

The completeness of the proposed holistic dark data governance maturity model was assessed through the evaluation of three sub-criteria: the scope, definitions, and perceived comprehensiveness. This assessment was conducted by analysing the participants' level of agreement with a series of five statements coded MCM1 to MCM5, in which participants used a Likert scale from 5 (strongly agree) to 1 (strongly disagree) to indicate their agreement or disagreement with each statement. The consensus of the participants' feedback on the statements to evaluate the completeness of the model is illustrated in Figure 7.2. The results show a general agreement among the participants for the given statements, completeness assessment with a consensus that exceeds 60 % for each statement.

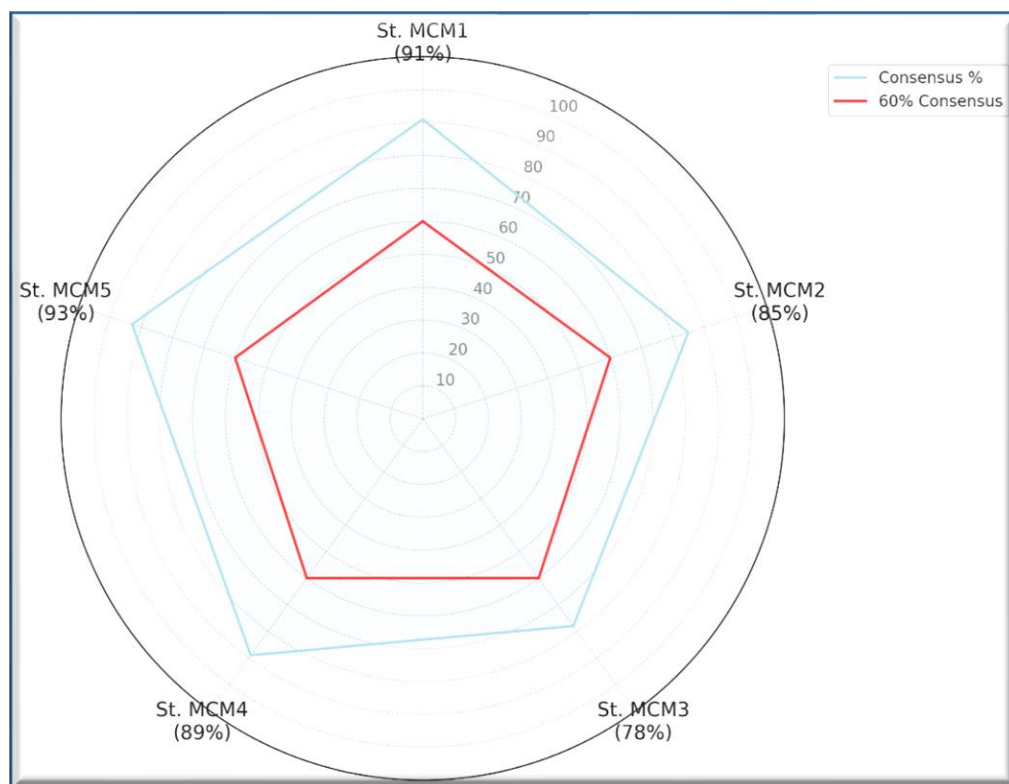


Figure 7. 2 The respondents' feedback for maturity model completeness

7.8.2. Consistency

This criterion aims to evaluate the level of consistency in the abstraction, granularity, and detail within the maturity model. The internal consistency of the maturity model has been used as the basis for this evaluation. The participants' level of agreement regarding the internal consistency

of the maturity model was investigated through a single statement: "There is a consistent level of abstraction, granularity, and detail given within the holistic dark data governance maturity model" coded as MIC1. The consensus of the participants' feedback on the statements to evaluate the consistency of the model is illustrated in Figure 7.3. The results show a general agreement among the participants for the given statement's consistency assessment with a consensus = 93%.

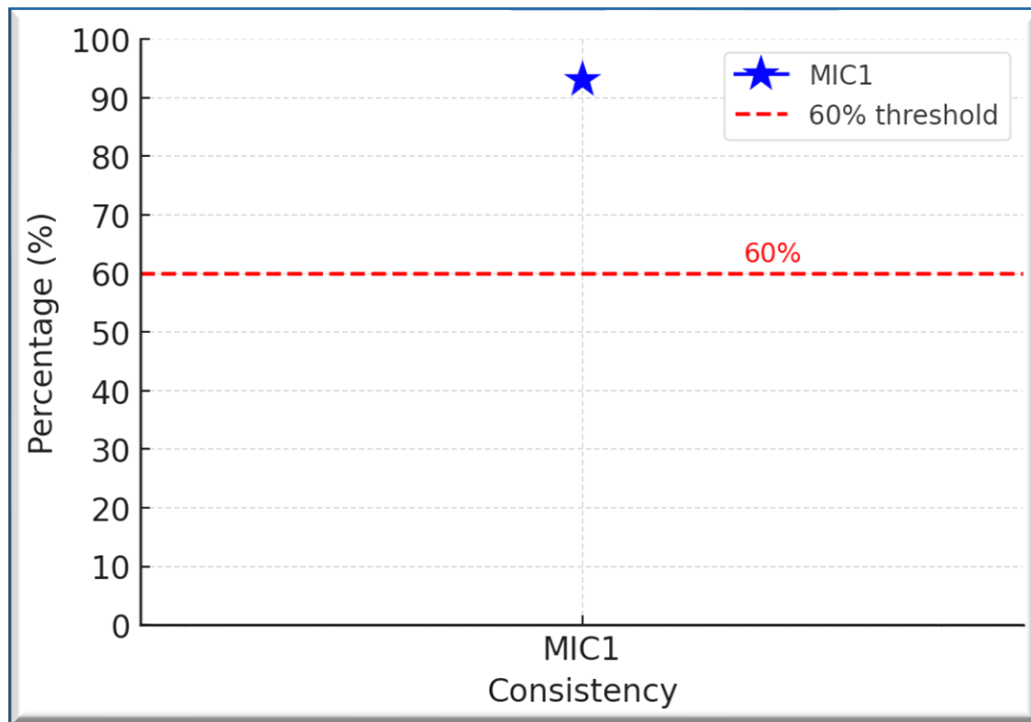


Figure 7. 3 The respondent's feedback on the maturity model's consistency

7.8.3. Practicality

This criterion evaluates the practicability of implementing the proposed holistic dark data governance maturity model, based on an assessment of five sub-criteria: the ease of use, the ease of learning, the understandability, the practical utility, and the tailorability of the model. The evaluation of the practicality of the model is accomplished through a series of five corresponding statements coded MPR1 to MPR5. The consensus of the participants' feedback on the statements to evaluate the practicality of the model is illustrated in Figure 7.4. The results show a general agreement among the participants for the given statements' practicality assessment with a consensus that exceeds 60 % for each statement.

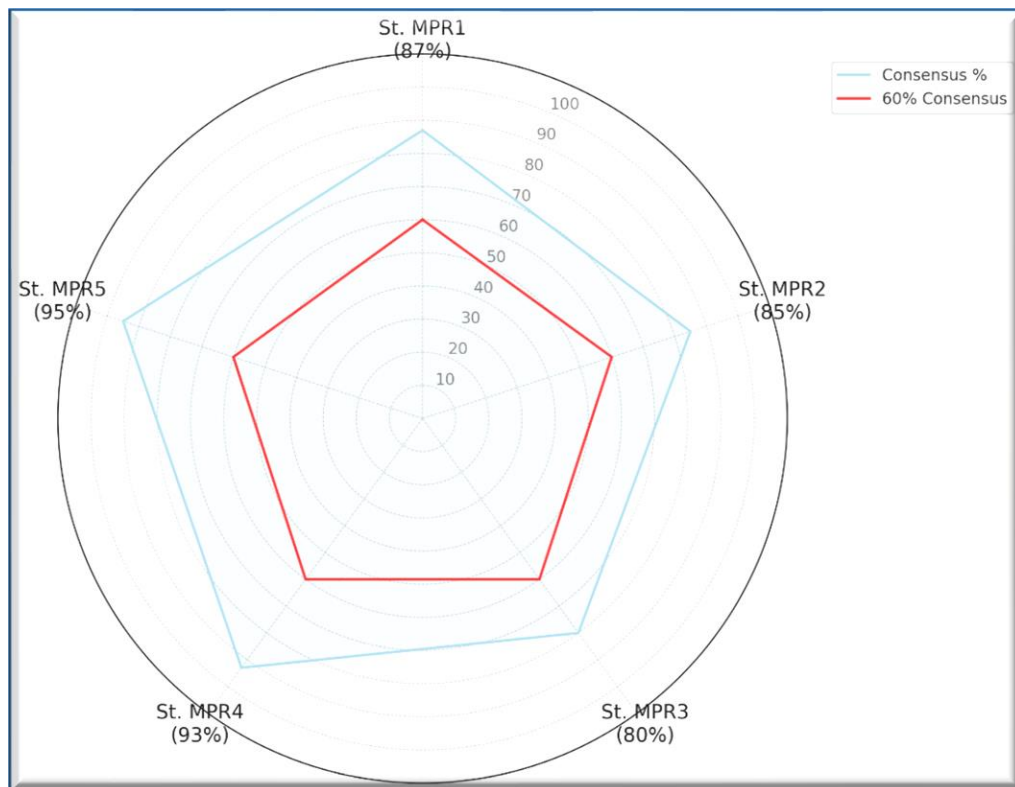


Figure 7. 4 The respondent's feedback on the maturity model's practicality

7.8.4. Usefulness

This criterion assesses the usefulness of the maturity model for evaluating and enhancing the organisation's dark data governance practices. It considers two factors: the perceived benefits and the model's constructiveness. The evaluation of the usefulness criteria is based on two corresponding statements coded MUS1 and MUS2, in which participants used a Likert scale from 5 (strongly agree) to 1 (strongly disagree) to indicate their agreement or disagreement with each statement. The consensus of the participants' feedback on the statements to evaluate the usefulness of the model is illustrated in Figure 7.5. The results show a general agreement among the participants for the given statements' usefulness assessment with a consensus that exceeds 60 % for each statement.

7.8.5. Verifiability

This criterion aims to assess the verifiability of the maturity model, considering three sub-criteria: feasible test coverage, stability, and verifiability. The evaluation of the verifiability criteria is based on three corresponding statements coded MVR1 to MVR3, in which participants used a Likert scale from 5 (strongly agree) to 1 (strongly disagree) to indicate their agreement or disagreement with each statement. The consensus of the participants' feedback

on the statements to evaluate the verifiability of the model is illustrated in Figure 7.6. The results show a general agreement among the participants for the given statements' verifiability assessment with a consensus that exceeds 60 % for each statement.

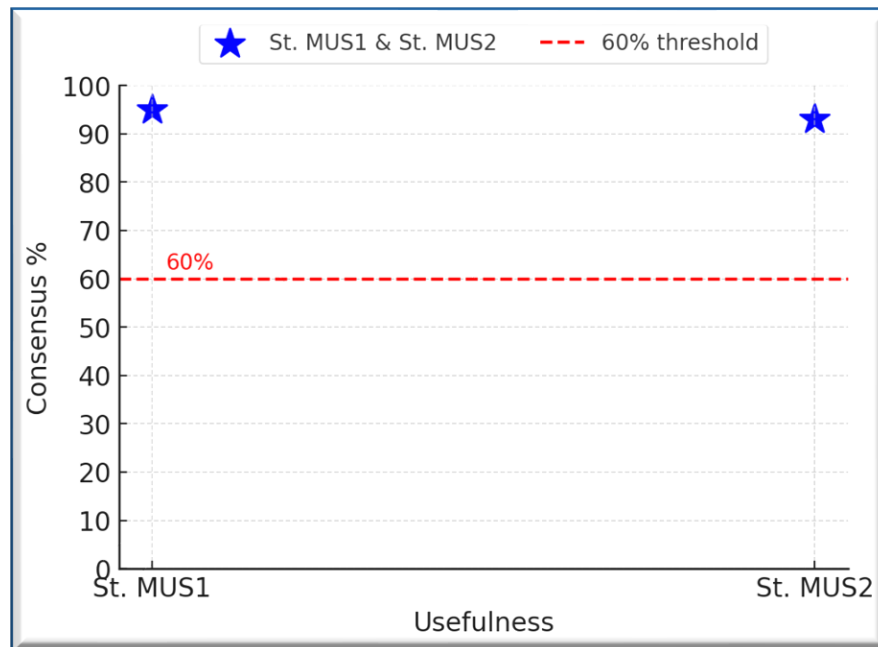


Figure 7. 5 The respondents' feedback on the maturity model's usefulness

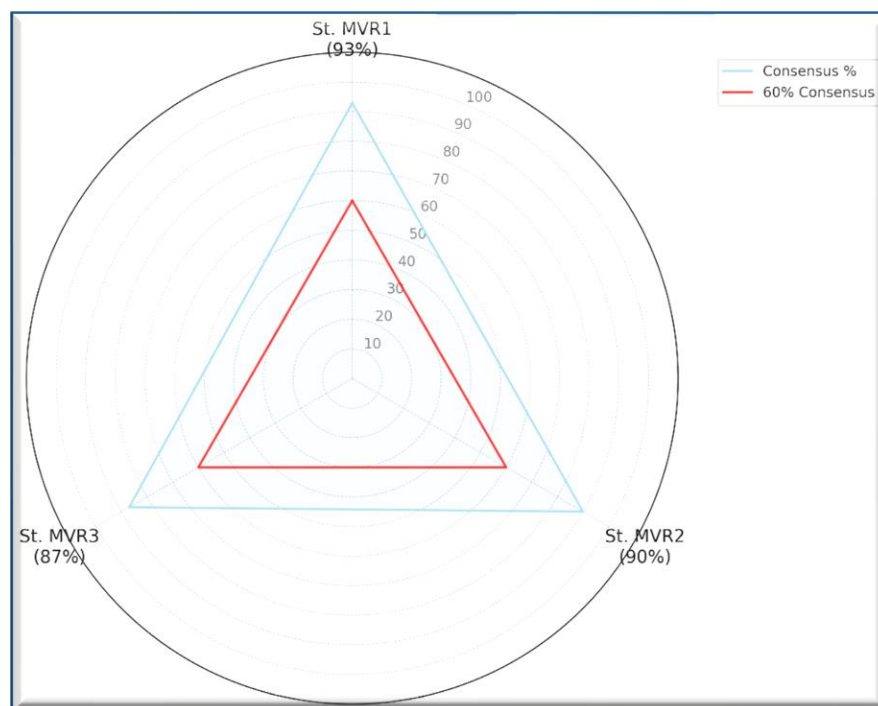


Figure 7. 6 The respondent's feedback on the maturity model verifiability

7.8.6. Participants' Recommendations to Improve the Proposed Maturity Model

In addition to the overall feedback from the expert panel and the general consensus among the participants regarding the proposed holistic dark data governance maturity model discussed in the previous section, the participants offered recommendations to enhance the model. The key suggestions were:

1. To replace the name of maturity level 5 from "innovate" with a more appropriate term that better reflects the intended meaning of that level. The majority of the participants recommended changing it to "viable" or "stable" to align better with the holistic nature of the model within the organisational context of the Viable System Model.
2. In alignment with the first point, update the descriptions of the other levels to incorporate the degree of support for organisational viability. As discussed in Chapter 4 (section 4.4), the context of supporting organisational viability means that the ultimate purpose of holistic data governance is generally seen as creating business value, while simultaneously mitigating dark data-related risks to support the achievement of organisational goals

Based on the above qualitative feedback, the levels proposed definitions in Chapter 5 (Section 5.4.2.3.) were modified as outlined in Table 7.2. Also, the maturity levels and the model were updated as depicted in Figure 7.7 and Figure 7.8.

Maturity Level Name	Description
Level 1: Initial (Ad-hoc)	Holistic Data governance (HDG) practices are informal, inconsistent, and reactive. There are no formal policies, and issues are addressed on an as-needed basis. Organisations at this stage often lack formal data governance structures and rely on individual efforts without cohesive oversight. HDG lacks the capability to support organisational viability.
Level 2: Developing (Defined)	Basic HDG policies are defined, but implementation is inconsistent. Data management responsibilities are assigned, but there may be gaps in enforcement. At this level, organisations start to formalize governance processes but often face challenges in maintaining consistency across departments and in supporting organisational viability.
Level 3: Managed (Proactive)	Data governance processes are well-defined and consistently applied. Governance policies are integrated into everyday business practices, with a focus on data quality and compliance. Organisations are proactive in managing data governance, using performance metrics to measure data

Maturity Level Name	Description
	quality, accessibility, and compliance. HDG is proactive in supporting organisational viability.
Level 4: Optimized (Predictive)	Data governance is fully integrated into the organisation's culture and processes. Advanced practices, like predictive analytics for data quality management and continuous improvement, are in place. Organisations use advanced analytics and automation to monitor and enhance governance practices continually to support organisational viability.
Level 5: Viable	Data governance is fully adaptive, allowing rapid responses to new data challenges and regulatory changes. Organisations continuously innovate and improve their governance frameworks. Data governance is deeply embedded into the culture and operationalized across all functions to fully support organisational viability.

Table 7. 2 Amended maturity levels' description after participants' feedback

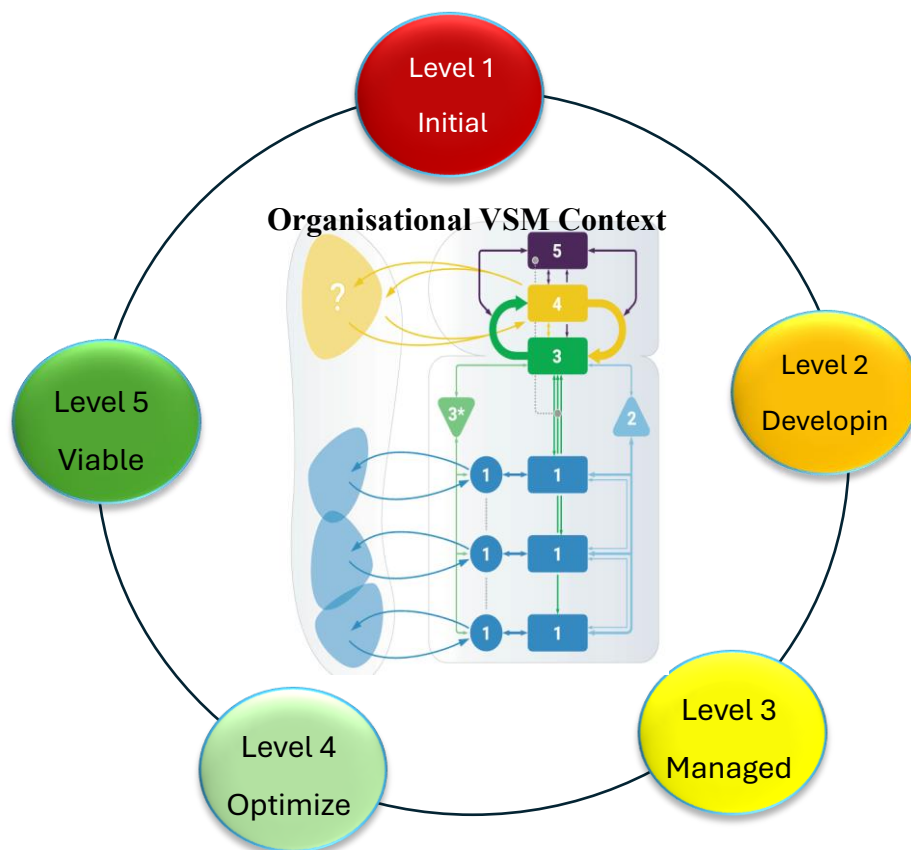


Figure 7. 7 Amended dark data governance maturity after participants' feedback

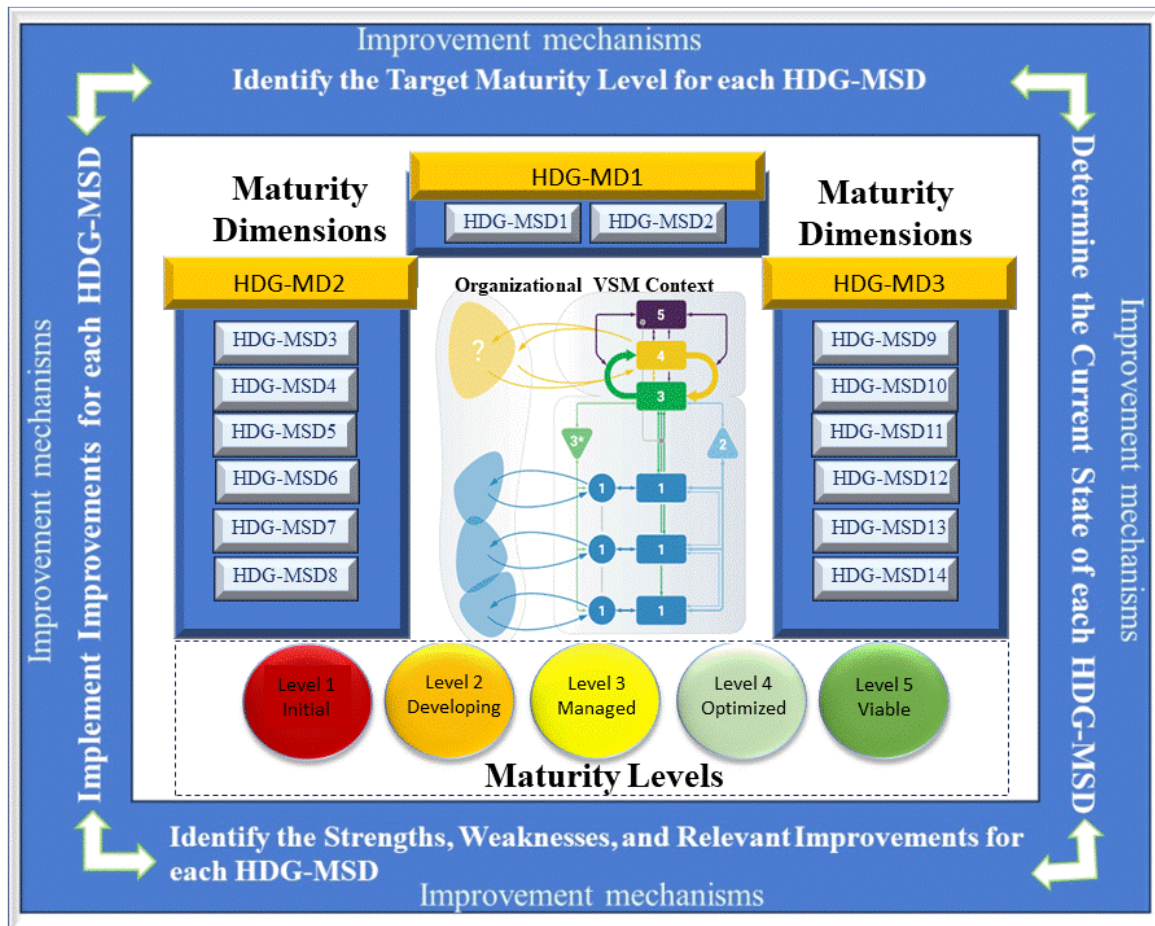


Figure 7. 8 Amended maturity model after participants' feedback

7.9. Holistic Dark Data Governance Assessment Matrix Evaluation

This study employed a comprehensive set of six criteria to thoroughly evaluate the proposed holistic dark data governance assessment matrix. These included evaluations of the matrix's completeness, consistency, practicality, usefulness, verifiability, and an analysis of its strengths and weaknesses. The assessment results were based on both quantitative and qualitative feedback obtained from the expert panel. A Likert scale was employed, where respondents indicated their level of agreement or disagreement with a series of statements about the assessment matrix. Figure 7.9 illustrates the overall evaluation process for the holistic dark data governance assessment matrix.

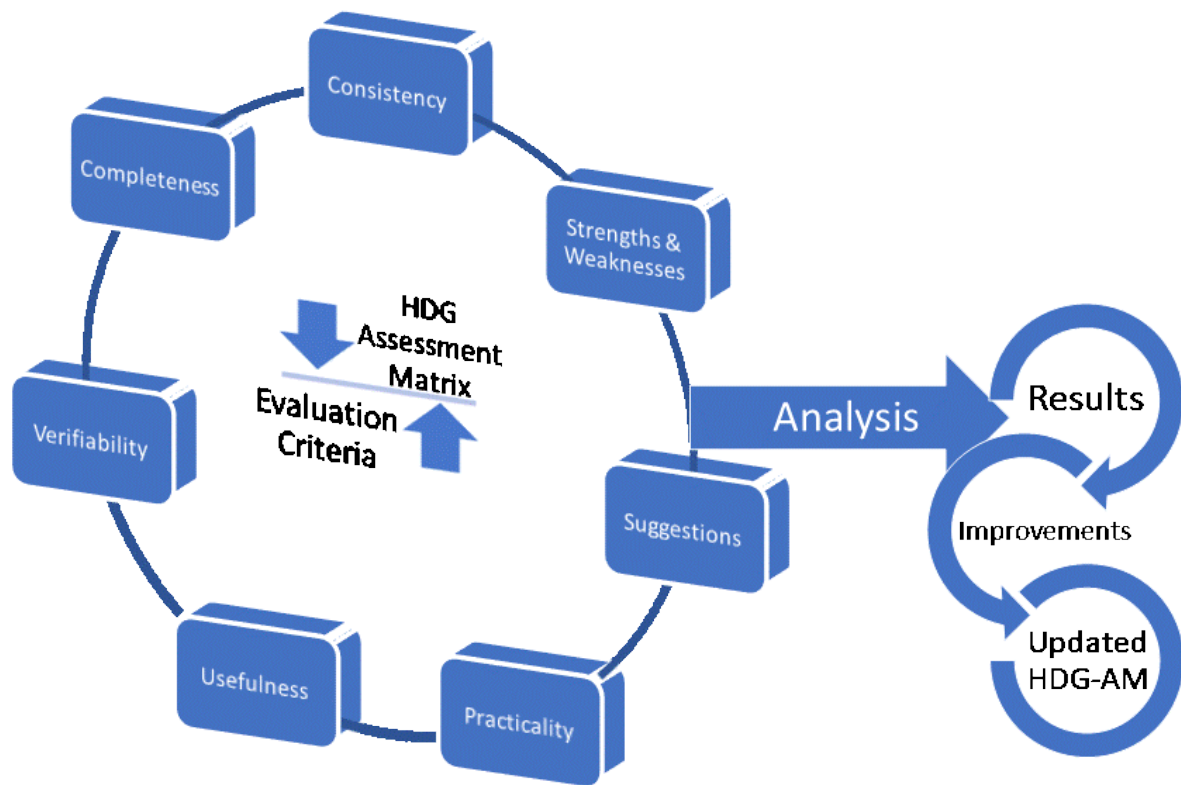


Figure 7. 9 The holistic dark data governance assessment matrix evaluation process

The results for each criterion are presented below:

7.9.1. Completeness

The completeness of the proposed holistic dark data governance assessment matrix was assessed through the evaluation of three sub-criteria: the scope, definitions, and perceived comprehensiveness. This assessment was conducted by analysing the participants' level of agreement with a series of four statements coded ACM1 to ACM4, in which participants used a Likert scale from 5 (strongly agree) to 1 (strongly disagree) to indicate their agreement or disagreement with each statement. The consensus of the participants' feedback on the statements to evaluate the completeness of the model is illustrated in Figure 7.10. The results show a general agreement among the participants for the given statements' completeness assessment with a consensus that exceeds 60 % for each statement.

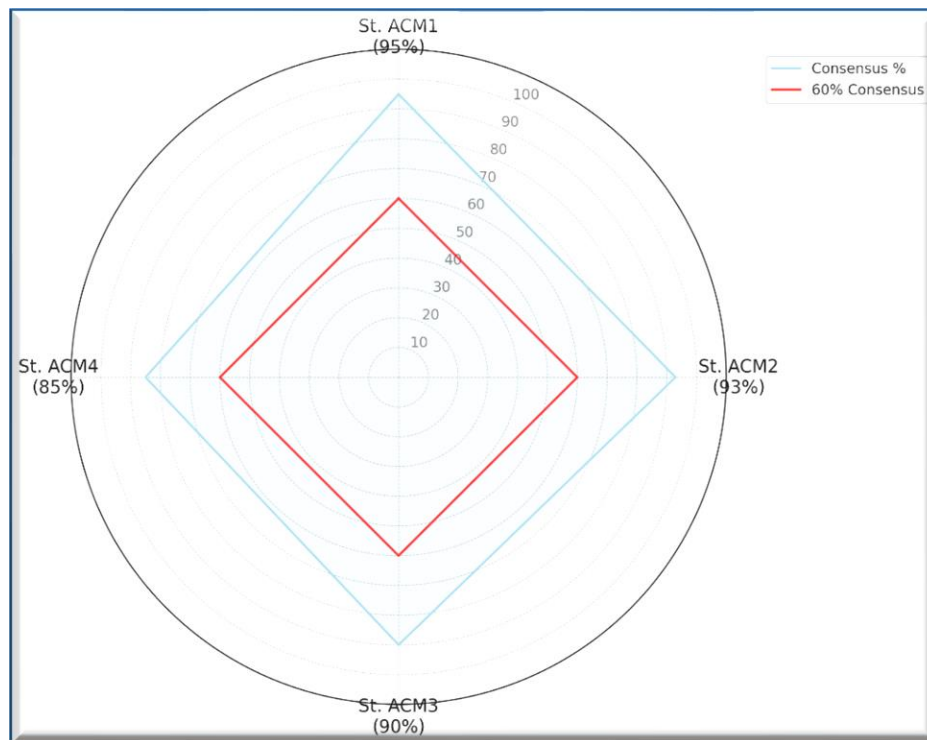


Figure 7. 10 The respondents' feedback for assessment matrix completeness

7.9.2. Consistency

This criterion seeks to evaluate the level of consistency in terms of abstraction, granularity, and detail within the assessment matrix. The internal consistency of the assessment matrix has been used as the basis for this evaluation. The participants' degree of agreement regarding the internal consistency of the assessment matrix was investigated through a single statement: "There is a consistent level of abstraction, granularity, and detail given within the holistic dark data governance assessment matrix" coded as AIC1. The consensus of the participants' feedback on the statements to evaluate the consistency of the model is illustrated in Figure 7.11. The results show a general agreement among the participants for the given statement's consistency assessment with a consensus = 95%.

7.9.3. Practicality

This criterion assesses the practicability of implementing the proposed holistic dark data governance assessment matrix, based on evaluating five sub-criteria: the ease of use, the ease of learning, the understandability, the practical utility, and the tailorability of the matrix. The assessment of the practicality criterion is accomplished through a series of five corresponding evaluation statements coded APR1 to APR5. The consensus of the participants' feedback on

the statements to evaluate the model's practicality is illustrated in Figure 7.12. The results show a general agreement among the participants for the given statements' practicality assessment with a consensus that exceeds 60 % for each statement.

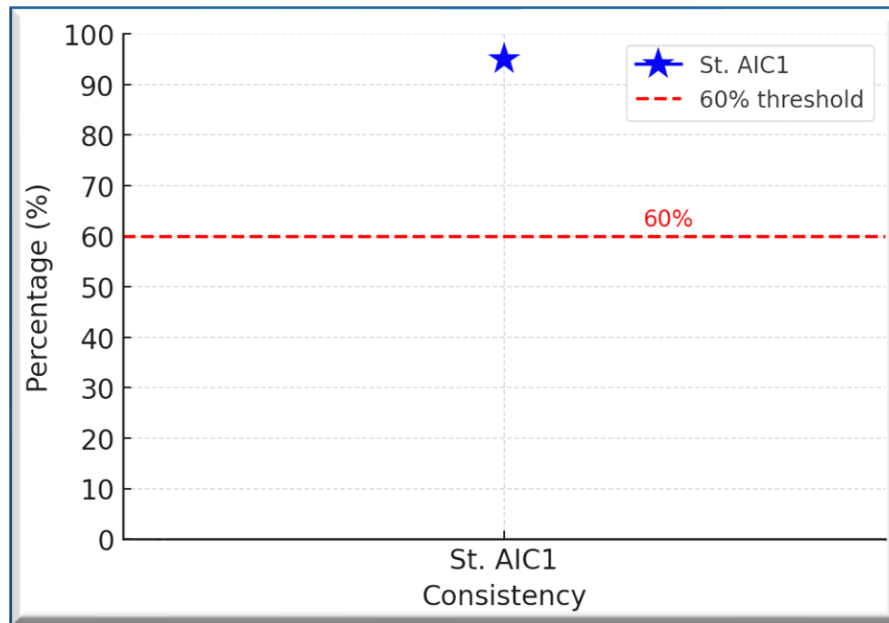


Figure 7. 11 The respondents' feedback for assessment matrix consistency

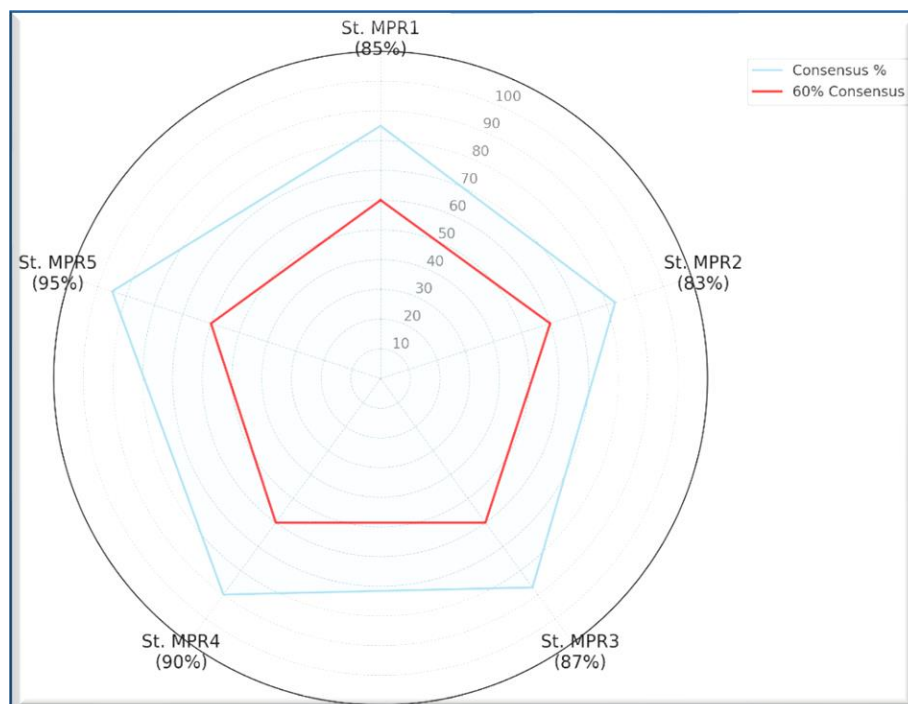


Figure 7. 12 The respondents' feedback for assessment matrix practicality

7.9.4. Usefulness

This criterion seeks to assess the utility of the assessment matrix for evaluating and enhancing the organisation's dark data governance practices. It considers two factors: the perceived benefits and the matrix's constructiveness. The evaluation of the usefulness criteria is based on two corresponding statements coded AUS1 and AUS2, in which participants used a Likert scale from 5 (strongly agree) to 1 (strongly disagree) to indicate their agreement or disagreement with each statement. The consensus of the participants' feedback on the statements to evaluate the usefulness of the model is illustrated in Figure 7.13. The results (AUS1=95% & AUS2=93%) show a general agreement among the participants for the given statements' usefulness assessment with a consensus that exceeds 60 % for each statement.

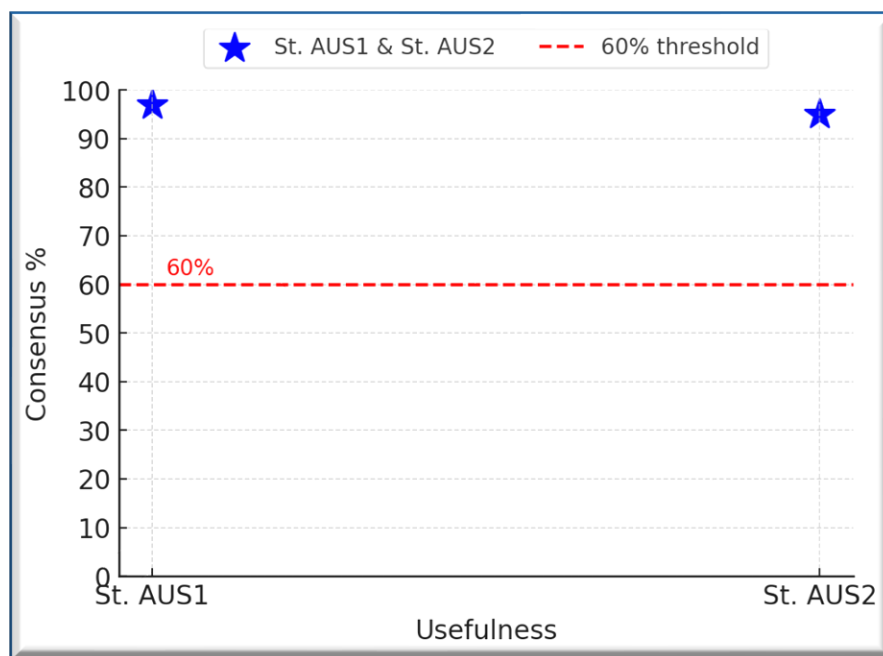


Figure 7. 13 The respondents' feedback on the usefulness of the assessment matrix

7.9.5. Verifiability

This criterion seeks to assess the verifiability of the assessment matrix by examining three sub-criteria: feasible test coverage, stability, and verifiability. The verifiability criteria are evaluated through a series of three corresponding statements coded AVR1 to AVR3, in which participants used a Likert scale from 5 (strongly agree) to 1 (strongly disagree) to indicate their agreement or disagreement with each statement. The consensus of the participants' feedback on the statements to evaluate the verifiability of the model is illustrated in Figure 7.14. The results

show a general agreement among the participants for the given statements' verifiability assessment with a consensus that exceeds 60 % for each statement.

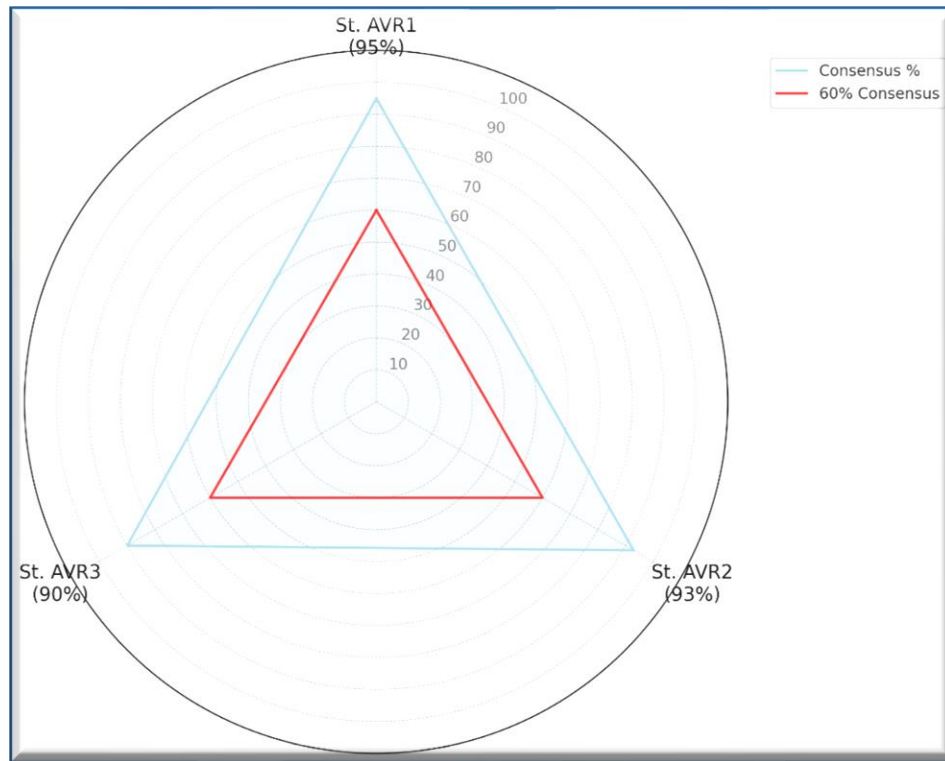


Figure 7. 14 The respondents' feedback on the verifiability of the assessment matrix

7.9.6. Strengths and Weaknesses

This criterion seeks to assess the strengths and limitations of the assessment matrix based on two sub-criteria: the individual level and the individual dimension within the assessment matrix. The participants utilized a Likert scale ranging from 5 (strongly agree) to 1 (strongly disagree) to indicate their level of agreement or disagreement with each statement, thereby rating the strengths and weaknesses of the assessment matrix.

7.9.6.1 Individual Maturity Level in Assessment Matrix

This criterion evaluates the merits and limitations of the content of the assessment matrix levels in measuring the systemic functions of the dark data governance holistic model. Five evaluation statements were employed to assess the strengths and weaknesses of the assessment matrix levels' contents, and these statements were coded LC.1 to LC.5, in which participants used a Likert scale from 5 (very Good) to 1 (Very Poor) to indicate their agreement or disagreement with each statement. The consensus of the participants' feedback on the statements about the

strengths and weaknesses of the assessment matrix levels' contents is illustrated in Figure 7.15 (Scores) and Figure 7.16 (Consensus %).

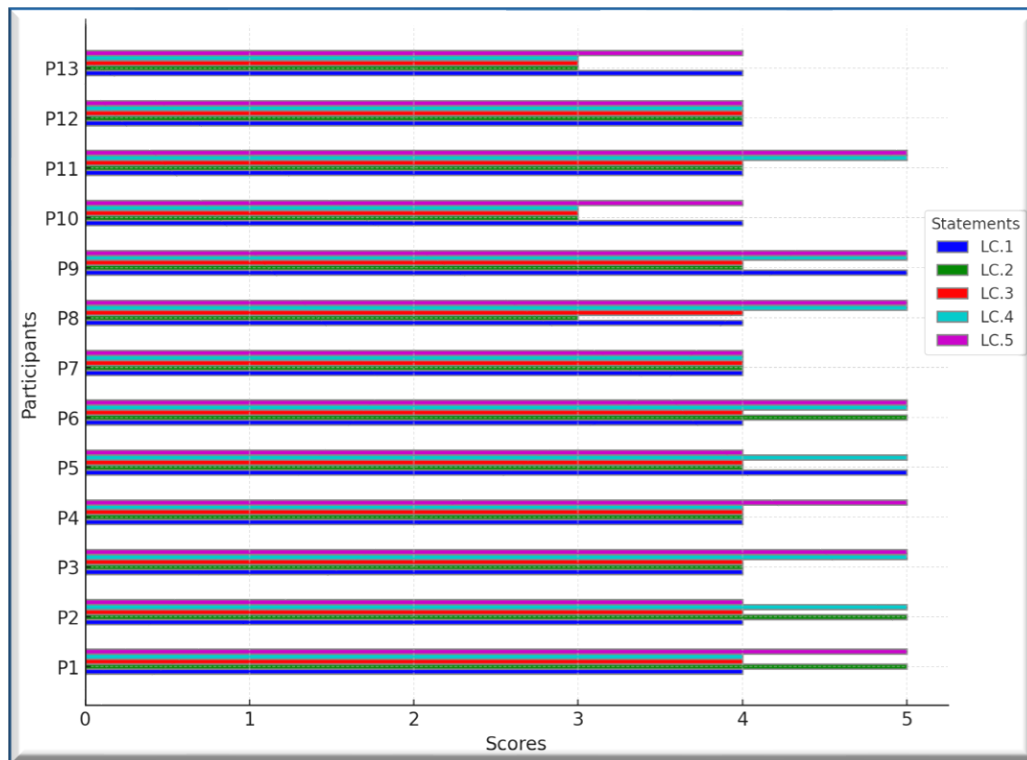


Figure 7. 15 The scores for the content’s strengths and weaknesses of the individual levels in the assessment matrix

The evaluation results depicted in Figures 7.15 and 7.16 indicate a robust overall consensus among the participants. Figure 7.16 illustrates a consensus exceeding 60% among the participants for each statement, signifying a high degree of collective endorsement. Likewise, Figure 7.15 reveals that the majority of participants provided ratings between 4 and 5 on the scale across all maturity levels, suggesting a strong approval of the assessment matrix. Statements like LC.1: “Level 1 in the assessment matrix provides strong content to measure the constructs of the holistic dark data governance maturity model”, LC.3: “Level 3 in the assessment matrix provides strong content to measure the constructs of the holistic dark data governance maturity model”, and LC.5: “Level 5 in the assessment matrix provides strong content to measure the constructs of the holistic dark data governance maturity model” show high consistency and consensus among the participants, with minimal variability, reflecting broad alignment and acceptance of the content within those levels of the assessment matrix. In contrast, LC.2: “Level 2 in the assessment matrix provides strong content to measure the constructs of the holistic dark data governance maturity model” and LC.4: “Level 4 in the

assessment matrix provides strong content to measure the constructs of the holistic dark data governance maturity model” exhibit more divergence, with scores ranging from 3 to 5, indicating some differing perspectives among the participants. Specifically, participants P8, P9, P10, and P13 provided more neutral ratings for those statements, suggesting they may have had some reservations or less certainty about the content within those levels. Despite this variability, the general trend across the evaluation statements shows a positive overall assessment, highlighting strong alignment among the participants and suggesting they largely agree with the statements regarding the strengths and weaknesses of the assessment matrix content.

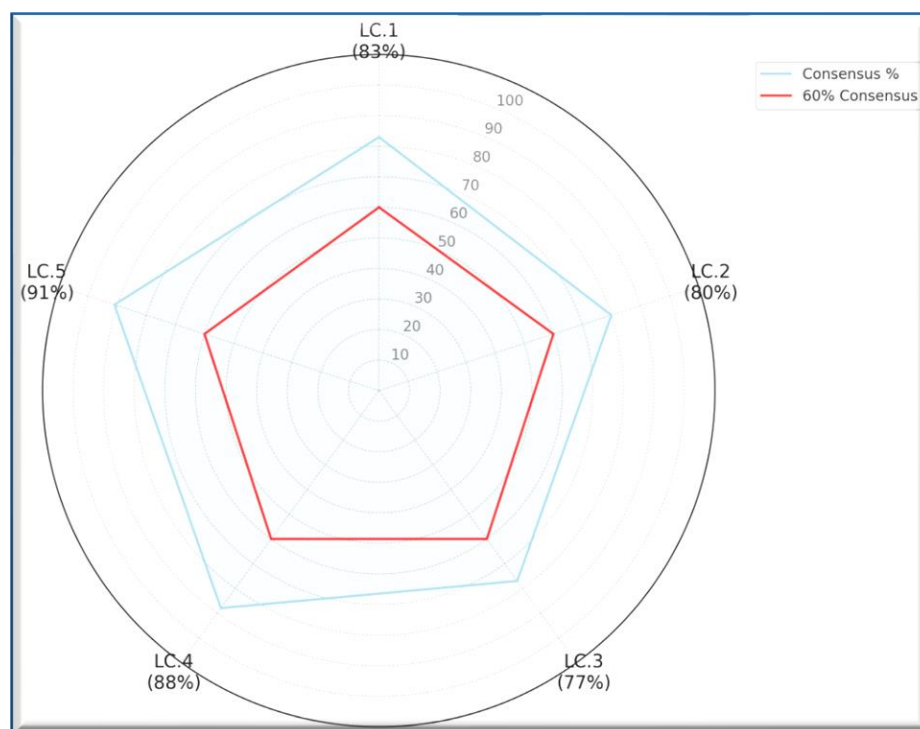


Figure 7. 16 The consensus% for the content’s strengths and weaknesses of the individual levels in the assessment matrix

7.9.6.2 Individual Maturity Dimension (Systemic Function) in Assessment Matrix

This criterion aims to assess the merits and limitations of the assessment matrix dimensions’ content in measuring the constructs of dark data governance. Fourteen evaluation statements were employed to gauge the strengths and weaknesses of the assessment matrix’s contents in measuring the constructs of the holistic dark data governance framework. These statements were coded DC.1 to DC.14, in which participants used a Likert scale from 5 (very Good) to 1 (Very Poor) to indicate their agreement or disagreement with each statement. The participants’

feedback on the statements about the strengths and weaknesses of the assessment matrix levels' contents is illustrated in Figure 7.17 (Scores) and Figure 7.18 (Consensus %).

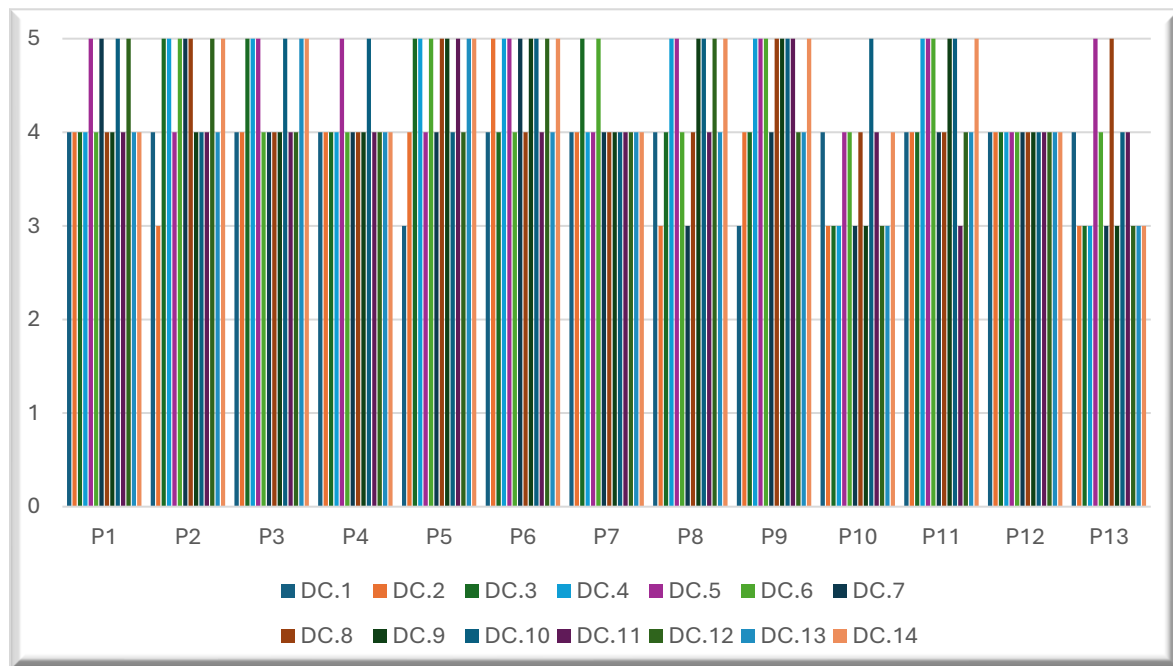


Figure 7. 17 The scores for the strengths and weaknesses of the individual systemic function in the assessment matrix

The evaluation results shown in Figures 7.17 and 7.18 indicate a robust overall consensus among the participants. Figure 7.18 illustrates a consensus exceeding 60% among the participants for each statement, signifying a high degree of collective endorsement. Likewise, Figure 7.17 reveals that the majority of participants provided ratings between 4 and 5 on the scale across all 14 statements, suggesting a strong approval of the individual systemic function in the assessment matrix. Some statements received consistently high scores, reflecting near-unanimous consensus among the participants like the following seven assessment statements:

- DC.5: The assessment matrix provides strong content to measure the “HDG-MSD5: Control Systemic Functions (SF3)” construct in the holistic dark data governance maturity model for each maturity level.
- DC.10: The assessment matrix provides strong content to measure the “HDG-MSD10: Requisite Variety Systemic Function (SF7)” construct in the holistic dark data governance maturity model for each maturity level.
- DC.4: The assessment matrix provides strong content to measure the “HDG-MSD4: Coordination Systemic Functions (SF2)” construct in the holistic dark data governance maturity model for each maturity level.

- DC.6: The assessment matrix provides strong content to measure the “HDG-MSD6: Auditing and Compliance (SF3) *” construct in the holistic dark data governance maturity model for each maturity level.
- DC.8: The assessment matrix provides strong content to measure the “HDG-MSD8: Strategic Direction and Feedback” construct in the holistic dark data governance maturity model for each maturity level.
- DC.12: The assessment matrix provides strong content to measure the “HDG-MSD12: Adaptability, Learning, and Change Management (SF9)” construct in the holistic dark data governance maturity model for each maturity level.
- DC.14: The assessment matrix provides strong content to measure the “HDG-MSD14: Transduction and Integration of All Systems (SF11)” construct in the holistic dark data governance maturity model for each maturity level.

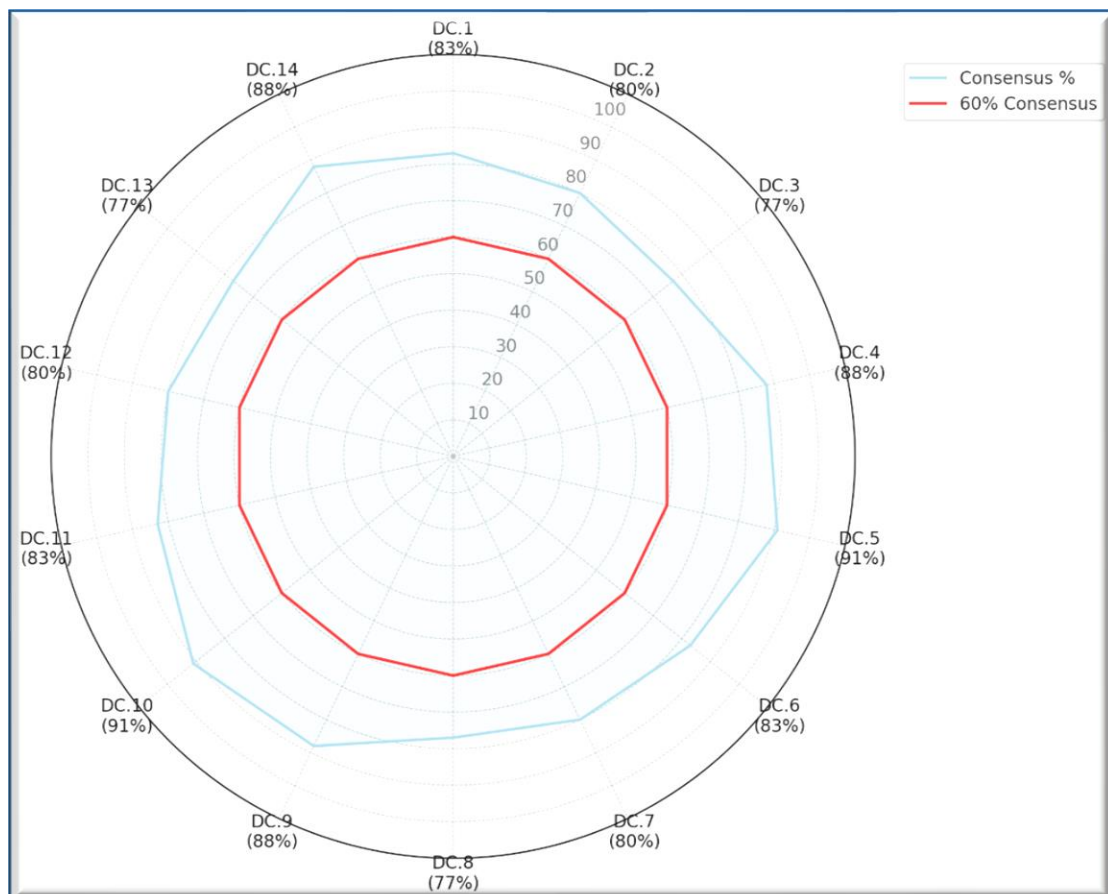


Figure 7. 18 The consensus% for the strengths and weaknesses of the individual systemic function in the assessment matrix

Other statements showed moderate consensus, with a mix of 3s, 4s, and 5s, such as the following five assessment statements:

- DC.1: The assessment matrix provides strong content to measure the “HDG-MSD1: VSM Organisational Context and Goals” construct in the holistic dark data governance maturity model for each maturity level.
- DC.2: The assessment matrix provides strong content to measure the “HDG-MSD2: Identifying Recursive Organisational Level and HDG Scope” construct in the holistic dark data governance maturity model for each maturity level.
- DC.3: The assessment matrix provides strong content to measure the “HDG-MSD3: Deployment Context Systemic Functions (SF1)” construct in the holistic dark data governance maturity model for each maturity level.
- DC.9: The assessment matrix provides strong content to measure the “HDG-MSD9: Recursivity Levels Integration (SF6)” construct in the holistic dark data governance maturity model for each maturity level.
- DC.11: The assessment matrix provides strong content to measure the “HDG-MSD11: Effective Inter-Operational Management (SF8)” construct in the holistic dark data governance maturity model for each maturity level.

This suggests that there were some differing perspectives among the participants regarding the effectiveness of the content within those particular assessment statements (dimensions).

The presence of neutral ratings (3s) indicates that there may be room for further refinement or clarification of the content in those areas.

The lowest consensus was found in:

- DC.9: The assessment matrix provides strong content to measure the “HDG-MSD9: Recursivity Levels Integration (SF6)” construct in the holistic dark data governance maturity model for each maturity level.
- DC.13: The assessment matrix provides strong content to measure the “HDG-MSD13: Communication Channels and Algedonic Channel (SF10)” construct in the holistic dark data governance maturity model for each maturity level.

These areas could benefit from potential revisions to better align with the participants' expectations and enhance the overall robustness of the assessment matrix.

Overall, the scores reflect a high level of agreement, with most participants rating all the statements positively. This indicates that the assessment matrix, as a whole, was well-received and viewed as a useful tool for evaluating the holistic dark data governance maturity model.

7.9.7. Participants' Recommendations to Improve the Proposed Assessment Matrix

In addition to the comprehensive feedback from the expert panel and the general consensus among the participants on the proposed holistic dark data governance assessment matrix, as discussed in the preceding section, the participants offered several recommendations to enhance the model. The key recommendations were as follows:

1. Adjust the maturity level 5 descriptions for all subdimensions to reflect the new name "Viable" of Level 5. This change was made to ensure that the highest level of the maturity model accurately captures the essence of an organisation's ability to sustain and continuously improve its dark data governance practices to support the viability of the organisation. Adjust other levels to reflect the level of support to organisational viability.
2. Develop an application tool to assess the state of an organisation's dark data governance in a real-world environment. This would help validate the effectiveness of the proposed framework and prove that it is working perfectly in practice.

The research carefully considered the recommendations provided by the participants. The first suggestion was taken into account and the relevant assessment tables in Chapter 5 were updated accordingly. The updated assessment matrices for HDG-MD1, HDG-MD2, and HDG-MD3, reflecting the participants' feedback, are presented in Table 7.3, Table 7.4, and Table 7.5 respectively.

However, the second recommendation to develop an application tool was not directly addressed in this research, as it was considered outside the primary scope of this study. Nevertheless, this suggestion has been included among the recommendations for future research in Chapter 8. Furthermore, the research incorporated a practical assessment by examining the application of the modified assessment matrix across realistic case scenarios at three leading universities in Texas, USA, to validate the feasibility and effectiveness of the model within an actual organisational context.

HDG-MD1: Sub-Dimensions / Levels	Level 1: Initial (Ad-hoc)	Level 2: Developing (Defined)	Level 3: Managed (Proactive)	Level 4: Optimized (Predictive)	Level 5: Viable (Adaptive)
HDG-MSD1: VSM Organisational	Holistic dark data governance goals are	Basic dark data governance goals are	Dark data governance goals are consistently	Holistic dark data governance is fully	Holistic dark data governance is highly

HDG-MD1: Sub-Dimensions / Levels	Level 1: Initial (Ad-hoc)	Level 2: Developing (Defined)	Level 3: Managed (Proactive)	Level 4: Optimized (Predictive)	Level 5: Viable (Adaptive)
Context and Goals	unclear and not aligned with the organisation's business context or strategic business objectives. The process is informal and reactive, providing little support for organisational viability or long-term planning within a systemic context.	defined, but alignment with broader organisational business goals is inconsistent. There are initial efforts to mitigate dark data-related risks and create business value, though this support for organisational viability is limited.	aligned with the organisational business context and strategic objectives. Integrated into business practices, focusing on mitigating dark data risks and supporting viability by proactively managing dark data in a systemic context.	integrated into the organisation's systemic business context. Goals are continuously refined, using predictive analytics to proactively manage dark data, thereby creating business value and ensuring the organisation's viability through strategic alignment.	adaptive, allowing rapid responses to new dark data challenges. Governance is deeply embedded into business strategic planning, continuously evolving to maximize business value and mitigate risks, ensuring the highest level of organisational viability.
HDG-MSD2: Identifying Recursive Organisational Level and HDG Scope	No identification of HDG scope or recursive business organisational level. Efforts are isolated at the top level, lacking a structured systemic approach. Consequently, there is little contribution to organisational viability or the creation of	Some recognition of HDG scope and recursive business levels is evident, though gaps exist in extending governance to the organisational context. Initial efforts to address dark data risks and support organisational	HDG scope and recursive organisational levels are clearly identified and incorporated into a structured systemic approach. The governance model supports business value creation by mitigating dark data risks across identified	Advanced methodologies monitor and adjust dark data governance scope at identified organisational levels, supporting viability by allowing the organisation to adapt to evolving risks and business needs while aligning governance	HDG scope is fully adaptive and defined organisation-wide, allowing real-time adjustments that maximize business value and support the achievement of operational and strategic goals. Governance evolves continuously to ensure

HDG-MD1: Sub-Dimensions / Levels	Level 1: Initial (Ad-hoc)	Level 2: Developing (Defined)	Level 3: Managed (Proactive)	Level 4: Optimized (Predictive)	Level 5: Viable (Adaptive)
	business value.	viability through governance are emerging.	levels, contributing to organisational viability.	with operational and strategic goals.	organisational viability within a systemic context.

Table 7. 3 Amended HDG-MD1 Assessment Matrix after participants' feedback

HDG-MD2: Sub-Dimensions / Levels	Level 1: Initial (Ad-hoc)	Level 2: Developing (Defined)	Level 3: Managed (Proactive)	Level 4: Optimized (Predictive)	Level 5: Viable (Adaptive)
HDG-MSD3: Deployment Context Systemic Functions (SF1)	Dark data governance deployment of systemic functions is informal and isolated. Dark data management is unstructured and disconnected from other governance domains, with no focus on supporting organisational viability.	Basic systemic functions of HDG are defined but implemented inconsistently across business units, with limited integration into other governance domains. Early efforts to support organisational viability exist but remain disjointed.	HDG systemic functions are well-defined and integrated into operational business units. They are aligned with other governance domains to support organisational viability, focusing on mitigating risks and creating business value.	HDG's systemic functions are fully integrated with business units, using advanced tools and predictive analytics to align with strategic objectives. Efforts proactively support organisational viability by optimizing performance and reducing dark data risks.	HDG systemic functions are fully adaptive and deployed across the organisation. Real-time adjustments enable the organisation to evolve with operational and strategic goals, ensuring long-term viability and business value creation.
HDG-MSD4: Coordination Systemic Functions (SF2)	Dark data governance coordination is reactive, and conflicts are managed as they arise.	Basic coordination functions exist but are inconsistent. Some alignment	HDG has well-defined coordination mechanisms to ensure compliance with policies	Advanced coordination mechanisms use predictive analytics to proactively address	Coordination mechanisms are fully adaptive and evolve with organisational changes. HDG

HDG-MD2: Sub-Dimensions / Levels	Level 1: Initial (Ad-hoc)	Level 2: Developing (Defined)	Level 3: Managed (Proactive)	Level 4: Optimized (Predictive)	Level 5: Viable (Adaptive)
	Compliance with HDG policies is minimal, with no alignment to support long-term organisational viability.	with corporate policies occurs, but gaps remain in ensuring HDG contributes to organisational viability.	and prevent conflicts, contributing to organisational viability by aligning governance practices with corporate goals.	conflicts. Full compliance with HDG policies supports organisational viability by ensuring alignment with corporate strategies.	policies are dynamically updated, ensuring continuous alignment with corporate strategies and external factors to enhance organisational viability.
HDG-MSD5: Control Systemic Functions (SF3)	Dark data governance control mechanisms are minimal, with limited oversight and no integration with other governance domains. This lack of control undermines efforts to support organisational viability.	Basic control mechanisms exist but are inconsistent, with fragmented integration into other governance domains. Initial efforts are made to support organisational viability through enhanced control.	Control functions are structured and integrated with other governance domains. A balanced approach supports self-regulation, aligning dark data governance with performance to contribute to organisational viability.	Advanced control mechanisms use automation and analytics to dynamically monitor compliance, resource allocation, and policy adherence, ensuring HDG supports organisational viability through data governance.	Control functions are fully adaptive, evolving based on feedback and organisational needs. HDG control mechanisms support long-term strategic goals and organisational viability by ensuring continuous alignment with business objectives.
HDG-MSD6: Auditing and Compliance (SF3*)	Dark data governance auditing and compliance functions are ad hoc, with limited mechanisms to gather data	Basic auditing processes are defined, but compliance evaluations are inconsistent. Initial steps are taken to	Systematic auditing and compliance evaluations are regularly conducted, informing governance practices and	Predictive analytics enhance auditing processes, providing real-time insights to ensure continuous	Adaptive auditing functions respond to new challenges, regulatory changes, and organisational needs.

HDG-MD2: Sub-Dimensions / Levels	Level 1: Initial (Ad-hoc)	Level 2: Developing (Defined)	Level 3: Managed (Proactive)	Level 4: Optimized (Predictive)	Level 5: Viable (Adaptive)
	on governance practices. There is no clear support for organisational viability through audits.	share audit results and begin corrective actions to support organisational viability.	driving corrective actions. This contributes to supporting organisational viability through continuous improvements in governance.	compliance and accuracy in governance practices, which support organisational viability.	Continuous feedback informs proactive adjustments, ensuring HDG compliance supports long-term organisational viability.
HDG-MSD7: Adaptation (SF4)	No formal processes exist to assess external changes. Dark data governance strategies are reactive, with minimal alignment to long-term goals or efforts to support organisational viability.	Initial efforts are made to assess external changes. Strategies are defined but inconsistently adapted to market analysis and environmental constraints, providing minimal support for organisational viability.	Formal adaptation functions are in place to assess external changes. Strategies are periodically updated to align with long-term goals and support organisational viability.	Predictive tools assess market trends and environmental changes. Strategies are proactively adjusted to maintain adaptability, enhancing organisational viability through responsive governance.	HDG strategies are fully adaptive, responding continuously to external changes. Long-term planning and market analysis dynamically inform governance functions, supporting organisational viability by aligning with evolving business goals.
HDG-MSD8: Strategic Direction and Feedback (SF5)	Decision-making for HDG is isolated, with no formal strategic direction or feedback mechanisms. There is no	Basic strategic direction is defined for HDG but is inconsistently applied. Feedback mechanisms are limited,	Strategic direction is clearly established, and feedback loops monitor and align HDG practices with organisational	Advanced decision-making processes use predictive analytics to inform strategic direction. Continuous	Strategic direction is fully adaptive, balancing internal and external perspectives. Real-time feedback informs

HDG-MD2: Sub-Dimensions / Levels	Level 1: Initial (Ad-hoc)	Level 2: Developing (Defined)	Level 3: Managed (Proactive)	Level 4: Optimized (Predictive)	Level 5: Viable (Adaptive)
	alignment with organisational goals, hindering efforts to support organisational viability.	resulting in minimal alignment between current and future governance states, affecting organisational viability.	goals. This supports organisational viability by ensuring governance evolves in response to business needs.	feedback ensures that governance practices dynamically align with corporate strategies, supporting organisational viability.	decision-making, ensuring HDG practices continuously align with short-term and long-term goals to support organisational viability.

Table 7. 4 Amended HDG-MD2 Assessment Matrix after participants' feedback

HDG-MD3: Sub-Dimensions / Levels	Level 1: Initial (Ad-hoc)	Level 2: Developing (Defined)	Level 3: Managed (Proactive)	Level 4: Optimized (Predictive)	Level 5: Viable (Adaptive)
HDG-MSD9: Recursivity Levels Integration (SF6)	No integration of governance domains (Data, IT, Corporate). Dark data challenges are addressed in isolation without considering the organisation's system as a whole, undermining efforts to support organisational viability.	Initial efforts to integrate governance domains exist, but they are fragmented and inconsistently applied across all levels of the organisation. Limited impact on mitigating dark data risks to support organisational viability.	Integration of governance domains is structured and aligned with the organisation's system, addressing dark data challenges proactively, thus contributing to business value creation and supporting organisational viability.	Full integration using advanced tools and analytics. Continuous monitoring aligns governance domains with organisational goals and external environments to mitigate dark data risks, enhancing organisational viability and performance.	Adaptive integration across all governance domains and levels, rapidly responding to internal and external changes. This ensures mitigation of dark data risks and supports the achievement of operational and strategic goals, ensuring organisational viability.

HDG-MD3: Sub-Dimensions / Levels	Level 1: Initial (Ad-hoc)	Level 2: Developing (Defined)	Level 3: Managed (Proactive)	Level 4: Optimized (Predictive)	Level 5: Viable (Adaptive)
HDG-MSD10: Requisite Variety Systemic Function (SF7)	No formal communication channels exist for identifying or addressing external dark data threats. The response to dark data requirements is reactive and disjointed, providing minimal support for organisational viability.	Basic communication mechanisms are established, focusing on present data requirements. Limited response to dark data threats and external disruptions, with only minimal contributions to organisational viability.	Proactive communication channels are established to identify and manage current and potential dark data threats. Governance processes adapt to emerging requirements, supporting organisational viability through risk mitigation.	Predictive analytics and advanced communication channels anticipate future data threats, ensuring systems adapt dynamically to required HDG changes. This proactive approach strengthens long-term goals and organisational viability.	Fully adaptive communication channels enable rapid identification and response to dark data threats. Continuous evolution ensures resilience to external digital dark data disruptions, supporting both operational effectiveness and organisational viability.
HDG-MSD11: Effective Inter-Operational Management (SF8)	No interaction between HDG operational units, coordination, and control functions. Operations lack autonomy and synergy, hindering organisational viability.	Initial interactions between HDG operational units, coordination, and control functions exist but are inconsistent, limiting synergy and responsiveness in mitigating dark data risks, thereby weakening organisational viability.	Defined interactions between operational units, coordination, and control foster self-regulation. HDG decision-making is improved through balanced autonomy and control, enhancing performance and	Predictive mechanisms enhance interactions between operational units, coordination, and control. Real-time insights improve decision-making, creating synergy between HDG functions and supporting	Fully adaptive interactions between HDG operational units, coordination, and control ensure dynamic decision-making. HDG operational autonomy and control are balanced to optimize performance and organisational viability,

HDG-MD3: Sub-Dimensions / Levels	Level 1: Initial (Ad-hoc)	Level 2: Developing (Defined)	Level 3: Managed (Proactive)	Level 4: Optimized (Predictive)	Level 5: Viable (Adaptive)
			supporting organisational viability.	organisational viability.	aligning with strategic goals.
HDG-MSD12: Metasystem Adaptability, Learning, and Change Management (SF9)	No HDG adaptability or learning mechanisms. Interactions among metasystem HDG systemic functions are absent, and change management is non-existent, undermining organisational viability.	Basic interactions among metasystem HDG systemic functions are established. Basic change management processes focus on short-term adaptations, with limited impact on continuous learning and organisational viability.	Established interactions among metasystem HDG systemic functions and change management processes. The organisation learns from dark data governance practices and adjusts accordingly, supporting long-term organisational viability.	Predictive tools support continuous learning and adaptability. Change management processes evolve dynamically to align with both operational and strategic perspectives within metasystem HDG functions, enhancing organisational viability.	Fully adaptive interactions within the metasystem HDG functions continuously support learning. Change management strategies evolve in response to HDG feedback, ensuring organisational viability through adaptability and strategic alignment.
HDG-MSD13: Communication Channels and Algedonic Channel (SF10)	No established communication channels for addressing dark data risks. High-risk scenarios are managed reactively without structured intervention, undermining organisational viability.	Basic communication channels exist but are inefficient in managing dark data risks. Algedonic channels are partially implemented, but their effectiveness is limited, weakening	Effective communication channels exist across all HDG systemic functions, enabling proactive management of dark data risks. Algedonic channels trigger rapid responses,	Advanced communication systems use predictive analytics to ensure swift responses to dark data risks. Algedonic channels dynamically adjust to manage varying levels of risk,	Fully adaptive communication networks enable real-time intervention to manage dark data risks. Algedonic channels seamlessly integrate to address high dark data risks,

HDG-MD3: Sub-Dimensions / Levels	Level 1: Initial (Ad-hoc)	Level 2: Developing (Defined)	Level 3: Managed (Proactive)	Level 4: Optimized (Predictive)	Level 5: Viable (Adaptive)
		organisational viability.	supporting organisational viability through improved risk management.	contributing to organisational viability and strategic goals.	ensuring operational success and long-term organisational viability.
HDG-MSD14: Transduction and Integration of All Systems (SF11)	No common language or understanding of data or dark data (Transduction) across the organisation. Dark data governance is fragmented, leading to silos and undermining organisational viability.	Initial transduction processes are in place, but integration across HDG systemic functions is limited. HDG communication and shared knowledge between business and data stakeholders are inconsistent, limiting organisational viability.	Structured transduction facilitates a shared language and cohesive operations regarding dark data management. Common knowledge reduces silos and dark data risks, supporting organisational viability.	Advanced transduction integrates all HDG systemic functions. Predictive analytics enhance cohesive operations, ensuring that common knowledge between stakeholders supports dark data risk mitigation and organisational viability.	Fully adaptive transduction and integration among HDG systemic functions promote organisational stability. Shared knowledge supports the mitigation of dark data risks, optimizing performance and supporting long-term organisational viability.

Table 7. 5 Amended HDG-MD3 Assessment Matrix after participants' feedback

7.10. Practical Evaluation of the Research Findings

To further evaluate the research outcomes and address the participant's recommendation, the study incorporated a practical assessment by examining the application of the assessment matrix across realistic case scenarios at three leading universities in Texas, USA (University X, University Y, and University Z) that were actively adopting general data governance practices but had not yet adopted a comprehensive approach to dark data governance. This real-world evaluation aimed to investigate the feasibility and effectiveness of the proposed holistic

dark data governance maturity model and assessment framework within an actual organisational context. The case studies provided valuable insights into how the model and associated tools could be applied in practice, highlighting their relevance and proven effectiveness in addressing holistic dark data governance challenges faced by these universities to identify necessary improvements.

Achieving **Level 5 (Viable)** in holistic data governance is crucial for universities like University X, University Y, and University Z because it ensures their long-term organisational viability. At this level, data governance is fully integrated with the institution's strategic goals, enabling proactive risk management, particularly in handling dark data, and fostering adaptability to external changes. A viable governance model supports sustainable resource use, compliance with regulatory standards, and continuous improvement through dynamic feedback loops. Ultimately, reaching Level 5 maturity allows these universities to optimize performance, enhance academic and research excellence, and remain resilient and competitive in an increasingly complex, data-driven environment.

Below are the practical evaluations for the three universities.

7.10.1. Case Scenario 1: University X

The first case study examines a large university with a student population exceeding 30,000 students, and more than 17,000 faculty and staff. Based on the assessment matrix questionnaire results, University X has been adopting certain holistic dark data governance measures and now intends to expand and further strengthen these initiatives in the near future. This is aimed at enhancing the institution's overall data management and governance capabilities, thereby mitigating dark data challenges and supporting its strategic objectives.

- **Analysis of the Current Level of Holistic Dark Data Governance in University X**

To assess the current state of the dark data governance implementation at University X, a selected panel of 11 experts was requested to evaluate all of the statements represented by the defined sub-dimensions of the holistic dark data governance maturity model. The average results for all participants of this evaluation are presented in Table 7.6, which outlines the current maturity levels for each sub-dimension of holistic dark data governance within the university.

Sub-Dimension	Maturity Level
HDG-MSD1	Level 3
HDG-MSD2	Level 2
HDG-MSD3	Level 3
HDG-MSD4	Level 3
HDG-MSD5	Level 3
HDG-MSD6	Level 2
HDG-MSD7	Level 2
HDG-MSD8	Level 3
HDG-MSD9	Level 3
HDG-MSD10	Level 2
HDG-MSD11	Level 3
HDG-MSD12	Level 2
HDG-MSD13	Level 3
HDG-MSD14	Level 3

Table 7. 6 The maturity level of holistic dark data governance in University X

- **Analysis of the Target Level of Holistic Dark Data Governance in University X**

Overall, University X operates between Level 2 (Developing/Defined) and Level 3 in most of the 14 sub-dimensions. While University X has established some foundational elements of holistic data governance, significant improvements (Details in Appendix P) are necessary to reach full viability (Level 5) as presented in Figure 7.19, particularly in the areas of adaptation, auditing, and recursive integration.

While the university has made progress in establishing foundational governance dimensions and aligning them with some strategic objectives, there are still areas that require improvement. Key gaps exist in the integration of governance domains across all organisational levels, proactive risk management, and continuous auditing and adaptation mechanisms. To reach Level 5 (Viable), University X needs to enhance its governance practices by implementing advanced tools, improving communication and coordination functions, and ensuring that data governance is fully aligned with both short-term operational needs and long-term strategic goals.

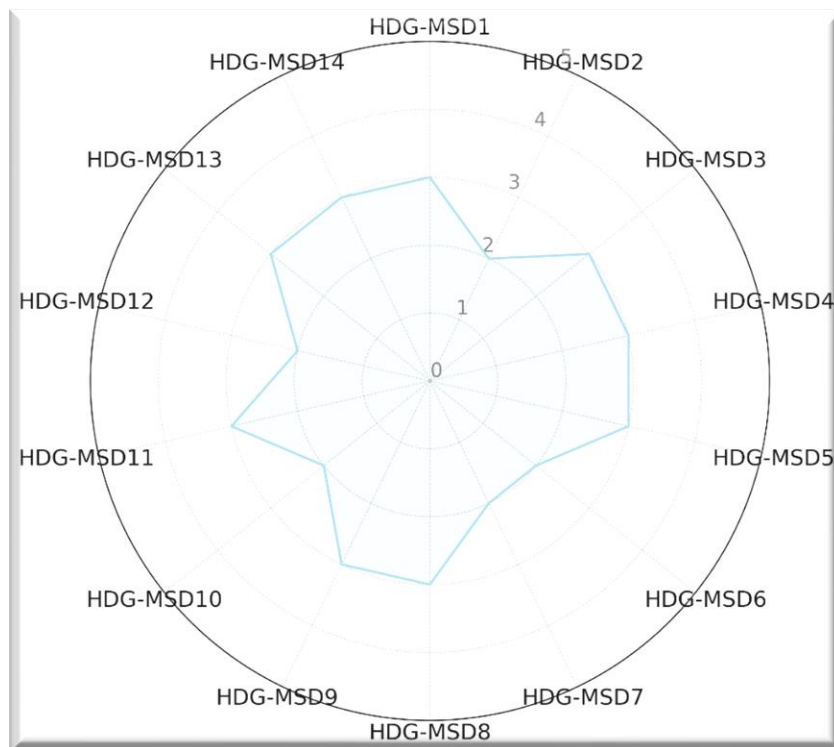


Figure 7. 19 The assessment of dark data governance in University X

7.10.2. Case Scenario 2: University Y

The second case study examines a large university with a student population exceeding 70,000 students, and more than 26,000 faculty and staff. According to the assessment matrix questionnaire findings, University Y has been implementing certain holistic dark data governance practices and now plans to expand and further strengthen these initiatives in the near future. This is aimed at enhancing the institution's comprehensive data management and governance capacities, thereby mitigating dark data challenges and supporting the achievement of the organisation's operational and strategic goals and objectives.

- **Analysis of the Current Level of Holistic Dark Data Governance in University Y**

To assess the current state of the dark data governance implementation at University Y, a selected panel of 11 experts was requested to evaluate all of the statements represented by the defined sub-dimensions of the holistic dark data governance maturity model. The average results for all participants of this evaluation are presented in Table 7.7, which outlines the current maturity levels for each sub-dimension of holistic dark data governance within the university.

- **Analysis of the Target Level of Holistic Dark Data Governance in University Y (Level 5)**

The overall maturity level for University Y is Level 2.5, reflecting a Developing/Managed state. While the university has established some data governance mechanisms, it needs to improve (Details in Appendix P) its systems as presented in Figure 7.20, particularly in the areas of coordination, control, adaptation, and communication, to progress toward viability.

Sub-Dimension	Maturity Level
HDG-MSD1	Level 3
HDG-MSD2	Level 2
HDG-MSD3	Level 3
HDG-MSD4	Level 2
HDG-MSD5	Level 2
HDG-MSD6	Level 2
HDG-MSD7	Level 2
HDG-MSD8	Level 3
HDG-MSD9	Level 2
HDG-MSD10	Level 2
HDG-MSD11	Level 3
HDG-MSD12	Level 2
HDG-MSD13	Level 3
HDG-MSD14	Level 3

Table 7. 7 The maturity level of holistic dark data governance in University Y

University Y demonstrates a developing to managed maturity in its holistic data governance across various departments. While the university has established data governance strategies, particularly in compliance, these efforts remain fragmented and inconsistently applied across all organisational levels. Key areas, such as auditing, coordination, and integration of governance functions across domains, are still reactive and lack proactive mechanisms for managing dark data risks. To achieve full maturity and full support to viability (Level 5), University Y needs to adopt advanced tools, and dynamic feedback systems, ensuring that governance strategies are continuously aligned with operational and long-term strategic goals. Enhanced synergy, adaptive learning, and the integration of governance across all organisational levels are essential to supporting fully matured viability.

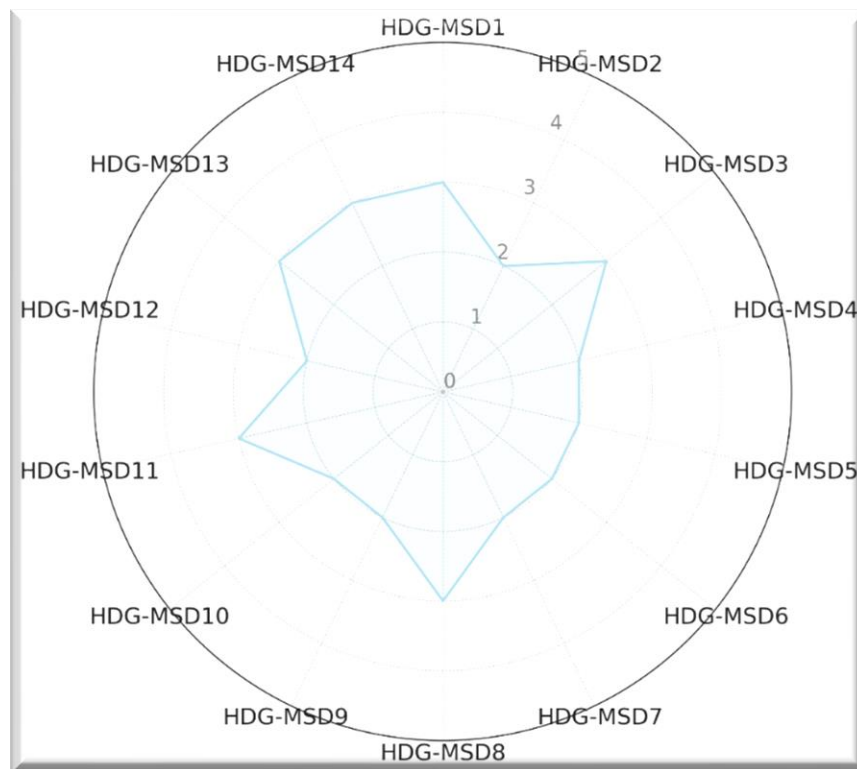


Figure 7. 20 The assessment of dark data governance in University Y

7.10.3. Case Scenario 3: University Z

The third case study examines a large university with a student population exceeding 47,000 students, and more than 18,000 faculty and staff. According to the assessment matrix questionnaire findings, University Z has been implementing certain holistic dark data governance practices and now plans to expand and further strengthen these initiatives shortly. This is aimed at enhancing the institution's comprehensive data management and governance capacities, thereby mitigating dark data challenges and supporting the achievement of the organisation's operational and strategic goals and objectives.

- **Analysis of the Current Level of Holistic Dark Data Governance in University Z**

To assess the current state of the dark data governance implementation at University Z, a selected panel of 11 experts was requested to evaluate all of the statements represented by the defined sub-dimensions of the holistic dark data governance maturity model. The average results for all participants of this evaluation are presented in Table 7.8, which outlines the current maturity levels for each sub-dimension of holistic dark data governance within the university.

Sub-Dimension	Maturity Level
HDG-MSD1	Level 2
HDG-MSD2	Level 2
HDG-MSD3	Level 3
HDG-MSD4	Level 2
HDG-MSD5	Level 3
HDG-MSD6	Level 2
HDG-MSD7	Level 2
HDG-MSD8	Level 3
HDG-MSD9	Level 2
HDG-MSD10	Level 2
HDG-MSD11	Level 3
HDG-MSD12	Level 2
HDG-MSD13	Level 3
HDG-MSD14	Level 3

Table 7. 8 The maturity level of holistic dark data governance in University Z

- **Analysis of the Target Level of Holistic Dark Data Governance HDG in University Z (Level 5)**

The overall maturity level for University Z is Level 2.5, reflecting a Developing/Managed state. While the university has established some governance mechanisms, key areas like adaptation, coordination, and communication need improvement (Details in Appendix P) to progress toward full maturity (Level 5) as presented in Figure 7.21.

University Z has made progress in establishing data governance practices, but significant gaps remain in fully aligning these with its strategic objectives. While some systemic functions are in place, governance is inconsistently applied across departments, limiting its ability to manage dark data risks effectively. Coordination and control mechanisms are fragmented, and auditing and compliance processes are reactive rather than proactive. To reach a higher level of maturity, University Z must enhance integration across all governance domains, deploy advanced tools, and implement continuous feedback mechanisms to ensure governance practices evolve in real-time, supporting operational and strategic goals. Achieving these improvements would position University Z to manage dark data risks more effectively, optimize decision-making, and ensure full support to organisational viability in a dynamic environment.

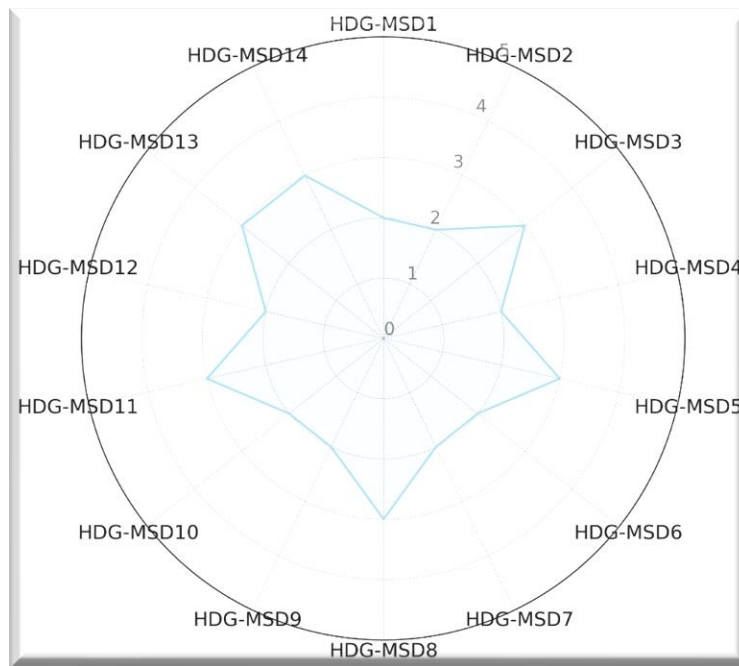


Figure 7. 21 The assessment of dark data governance in University X

7.11. Chapter Summary

This chapter has presented the evaluation results of the proposed holistic dark data governance maturity model and the evaluation of the assessment matrix using a rigorous Delphi approach. The findings from the panel of expert participants strongly supported the proposed concept, structure, and overall applicability of both the maturity model and the assessment matrix. The feedback and constructive comments gathered during the evaluation process have been reviewed and incorporated, leading to revisions and refinements in the original maturity model diagram. Similarly, adjustments were also made to the content and structure of the assessment matrix to reflect the participants' insightful suggestions and enhance its practical relevance and usefulness. To further test the real-world practicality and effectiveness of the proposed holistic dark data governance framework, maturity model, and assessment matrix, three case scenarios were employed and examined across 3 key universities in Texas, USA. These real-world case scenarios provided valuable insights into how the holistic model and associated tools could be effectively applied in actual organisational settings, showcasing their strong relevance and proven effectiveness in addressing critical dark data governance challenges to ultimately help organisations achieve their operational and strategic goals. The next chapter will present the overall research conclusions, summarize the key academic and practical contributions, and offer recommendations for future research work in this important domain.

Chapter 8: Research Conclusions and Recommendations

8.1. Introduction

This Chapter presents a summary of the research process and findings of this thesis. It begins with a research overview. This is followed by a summary of the key research findings and the study's contributions to the existing body of knowledge in the field. The chapter then delves into the research limitations, acknowledging the constraints and challenges encountered during the investigation. Finally, the chapter concludes with a set of well-thought-out recommendations for future research directions, offering valuable insights and opportunities for further exploration of the topic.

8.2. Research Overview

In the current digital landscape, dark data poses one of the most critical risks that organisations must manage to achieve their operational and strategic objectives. Despite the substantial benefits associated with dark data management, its deployment remains limited due to a range of issues and challenges. The key issues centre around the lack of control over data, the risks to data security and privacy, difficulties in ensuring data quality and reliability, and the ambiguous connection to the organisation's strategic objectives—all of which are crucial elements of data governance. Consequently, this thesis proposes a holistic dark data governance as a crucial reference model. This model requires rigorous and systemic data governance functions within a holistic organisational context, which can be more complex but necessary. However, the existing literature lacks substantial research on data governance for dark data management, despite its significance and the potentially catastrophic consequences of its mismanagement.

The purpose of this research was to develop a holistic model that could be used to design, implement, and sustain an effective dark data governance model within the holistic organisational context. Additionally, this study aimed to advance research in this field, which will contribute to the broader Information Systems and data management research communities and practitioners, with a particular emphasis on key universities in Texas, USA. To fulfil the research objectives outlined in Chapter One, a mixed research methodology was adopted, incorporating both Quantitative and Qualitative methods, including the analysis of relevant literature using a Systematic approach, Questionnaires, and the Delphi Approach. These combined with the adopted underlying theoretical basis and tools have all supported a rigorous research process, resulting in robust findings that meet the thesis' objectives. The following

section presents a summary of the research findings and their contribution to knowledge. This research is structured around four key directions that shape its contributions:

1. This study seeks to address the dark data governance challenge faced by prominent universities in Texas, USA. However, given the novel and unprecedented nature of this work, and the lack of a universal solution, it is crucial to first develop a holistic and integrated model for dark data governance. This model will facilitate an understanding of the essential phases and systemic functions necessary to enable the implementation of an effective dark data governance system within the broader organisational context.
2. To assist organisations in implementing their dark data governance model, developed within the holistic context of the organisation, there is a need for tools that allow them to evaluate their current state and establish their desired targets. Accordingly, a Maturity Model was proposed, accompanied by an assessment matrix.
3. This thesis emphasizes the integration of data governance, IT governance, corporate governance, other pertinent governance domains and business domain within a holistic systemic context to mitigate the risks associated with dark data. Such integration is crucial for organisations striving to achieve both operational and strategic goals within a holistic organisational context. By aligning these domains, organisations can ensure seamless information flow, improve decision-making processes, and enhance accountability across all operational levels. Together, these interconnected domains create a cohesive system that enhances organisational resilience, fosters innovation, adaptability, continuous learning, and drives sustainable growth.
4. The proposed models and frameworks were developed through a thorough review of the existing literature and grounded in relevant theoretical foundations, including Analytic Theory, Critical Success Factors, Viable System Model theories, and Cybernetics. As a result, the findings of this research could be applied to a broader range of contexts. However, given the specific focus of this thesis on addressing the dark data governance challenge for key universities in Texas, USA, it is crucial to further validate and evaluate the developed Holistic Model, Maturity Model, and Assessment Matrix by applying them to other industries beyond the educational sector to enhance their generalizability and practical relevance.

8.3. Summary of the Key Research Findings and Contributions

This research has yielded several key findings and contributed substantially to the domain of knowledge, particularly in the realm of holistic dark data governance. The major outcomes and scholarly contributions of this thesis are detailed as follows:

- **Gap Identification and Scope Definition:** This study has successfully identified research gaps within the existing literature, providing a critical evaluation of the state of data governance, particularly dark data governance. The research has led to novel contributions in this area, particularly emphasizing the necessity for a holistic approach in the rapidly evolving field of data governance. The implications of these findings are profound, potentially influencing both the academic community and practitioners globally, especially given the current scarcity of comprehensive research in holistic dark data governance.
- **State of the Art Evaluation:** A thorough evaluation of the state of the art of data governance and, more specifically, in dark data governance, including the identification of Critical Success Factors (CSFs) and Challenges to implementing effective dark data governance initiatives in organisations. A tertiary systematic literature review guideline has been undertaken in this research to understand the state of the art of data governance and dark data governance. The findings confirmed that currently there is no single approach to the implementation of data governance initiatives in all organisations, the findings were presented in Chapter Three. The impact of the results from the study could be significant for organisations in different countries and more specifically in USA. This is justified by the lack (almost no previous related work) of research and development and practice on data governance for dark data management. The Critical Success Factors (CSFs) and Challenges to implementing effective dark data governance initiatives in organisations were identified and classified based on in the literature findings, and they were presented in Chapter Three. Furthermore, based on the results findings in Chapter Three, a dark Data Governance Systemic Functions were developed in Chapter Four to support a model development.
- **Holistic Model Development:** A novel holistic model was developed to guide the design, deployment, and sustainability of effective dark data governance system. The model was presented in Chapter Four. This research developed a novel holistic model to address the identified gap in the existing literature, which was the lack of a comprehensive reference model to guide the design, deployment, and sustainability of effective dark data governance initiatives. The proposed model was grounded in analytical theory, critical success factors,

Viable System Model theories, and cybernetics principles. This model can assist decision-makers in understanding the essential systemic functions required to develop a robust dark data governance system, thereby helping key universities in Texas, USA, mitigate the risks associated with dark data and implement an effective holistic dark data governance approach. The model encompasses various systemic functions, including operational, coordination, control, intelligence, policy, recursion, requisite variety, and the balance of autonomy and control within the Viable System Model context. The model emphasizes organisational adaptability, continuous learning, and the balance between autonomy and control to counteract dark data risks and ensure organisational viability and the achievement of its goals. Additionally, the research outlines a methodology for implementing, deploying, and sustaining the model within the organisational Viable System Model context, focusing on defining the system-in-focus, assessing subsystems and their interactions, and ensuring continuous improvement. This approach aims to enhance decision-making, manage dark data risks, and support organisational viability and stability.

- **Maturity Model Development:** Addressing the identified gap regarding the absence of a maturity model, this research has formulated a dark data governance maturity model, which was presented in Chapter Five. A dark data governance maturity model was developed based on systemic functions of the holistic dark data governance model in Chapter Four, and maturity levels. The maturity model encompasses five distinct levels, ranging from an initial state of immaturity (level one) to a fully mature state (level five). This model aims to assist organisations in assessing their current level of dark data governance implementation and mapping out a strategic path toward achieving full maturity. This will be accomplished by classifying the various components of the holistic dark data governance model's systemic functions based on the five maturity levels. This is crucial for managing the complexities of dark data governance and achieving operational and long-term organisational goals.
- **Assessment Matrix Development:** Complementing the maturity model, a holistic dark data governance assessment matrix has been developed to help organisations gauge their current versus target states of governance, and it was presented in Chapter Five. This research developed a holistic dark data governance assessment matrix to complement the holistic dark data governance maturity model presented in this thesis. The assessment matrix was designed to help organisations identify their current state of dark data governance in relation to the target state, with the aim of enhancing dark data governance outcomes. The holistic dark data governance assessment matrix also enables organisations

to understand the strengths and weaknesses of their dark data governance, providing actionable insights and guidelines for improvement. The research adopted a mechanism to determine the best and worst practices, and then to characterize the various levels between them. The assessment matrix was constructed with five distinct levels, and fourteen cross-reference categories were incorporated for these levels. Additionally, the text descriptions for each level in the assessment matrix were formulated using terms such as "does not exist", "basic", "effective", "Advanced", and "fully adaptive" to differentiate the different stages of maturity.

- **Validation and Evaluation of Research Outcomes:** The outcomes of the research were validated and evaluated through rigorous processes, as summarized below:
 - To validate and evaluate the proposed model in Chapter Four, a Delphi study was conducted. The expert panel consisted of thirteen participants from a key university in Texas, USA. The findings indicated that the panel of experts agreed on the significance of the proposed model in developing a holistic dark data governance system within the organisational context. Additionally, the participants provided valuable recommendations to enhance and refine the proposed framework, and these suggestions were incorporated into the final version. The validation results are presented in Chapter Six.
 - The proposed maturity model and assessment matrix in Chapter Five were evaluated through a Delphi study involving a panel of thirteen experts from a key university in Texas, USA. The findings presented in Chapter Seven indicated that the panel agreed on the significance of the proposed maturity model and assessment matrix in assessing the holistic dark data governance model. Additionally, the participants provided valuable recommendations to enhance and refine the proposed maturity model and assessment matrix, and these suggestions were incorporated into the final versions. Furthermore, three case scenarios involving key universities in Texas were used to examine the practical application of the holistic dark data governance model in real-world settings. The findings presented in Chapter Seven indicated that the dark data governance implementation in the examined case scenarios demonstrated ongoing efforts by the organisations to progress toward their targeted governance objectives.

These structured validations and evaluations underscore the practical relevance and robustness of the research findings. Overall, this thesis not only advances theoretical frameworks in dark data governance but also offers practical models and tools that can be adapted by organisations

seeking to enhance their governance systems. The strategic incorporation of holistic dark data systemic functions within the organisational VSM context and the focused development of maturity and assessment models provide a foundational contribution to both the academic field and practical implementation in organisations.

8.4. Research Limitations

Although this thesis successfully met all research objectives, the author acknowledges certain limitations were partially addressed in this research and the rest could be addressed in future work. As the first study to explore holistic dark data governance on this scale, the absence of prior research in this area was both a benefit and a constraint. On the one hand, the lack of existing studies allowed for the development of an original and innovative framework. On the other hand, the findings could have been further enriched by a broader body of literature. A more developed literature base would have provided established methods, theories, models, and frameworks to guide the research direction. Additionally, the absence of a dedicated research community in holistic dark data governance limited the opportunity for peer engagement, which could have provided valuable feedback throughout the study. On the other hand, the lack of prior studies has given the Author the opportunity to establish some important foundations in the field of holistic dark data governance with invaluable contributions to knowledge.

This research recognized additional limitations associated with the Delphi study method, which can potentially affect the validity of the findings. A key limitation is the potential for bias in the selection of experts, as the credibility of the study depends on the expertise and diversity of the panel. The lack of interaction between experts can also hinder effective communication, as panelists may question whether their ideas were fully understood. Additionally, the wording of the questionnaire may lead to biased responses if experts answer based on what they believe the researcher wants. Furthermore, the varying levels of experience among experts can affect the quality of the responses and the credibility of the results. The iterative nature of the Delphi method, requiring multiple rounds, can be time-consuming, potentially leading to participant fatigue and dropout, which may influence the study's outcomes. Finally, maintaining anonymity throughout the process can present challenges, further complicating the study's integrity. Chapter 2 provided a detailed discussion of measures to mitigate the limitations associated with the research methodology. In this thesis, the sample population was suitable for the scale of the study and included a balanced representation from a key university in Texas,

USA. Participants came from varied roles, including senior leadership, specialized governance, and academia, with diverse experiences in governance. While this provided a comprehensive understanding of the university's governance practices, further validation of the proposed models across more universities in the USA would enhance the robustness of the findings.

This study was limited to examining holistic dark data governance at the level of the organisational Viable System Model's recursive level. The recursive nature of the Viable System Model suggests that organisations operate across interconnected levels, each reflecting a different scope of details but having similar governance systemic functions, and roles, with additional interactions across the levels. Therefore, limiting the study to one level restricts the exploration of how holistic dark data governance functions across various organisational levels. Further research conducted at other recursion levels would significantly enhance the understanding of how holistic dark data governance can be applied in a more integrated and dynamic manner.

A related limitation concerns participants' contributions to the study, which were affected by the lack of prior research in holistic dark data governance. Despite occupying senior positions such as IT Managers and Directors, some participants lacked deep expertise in this emerging field. To mitigate potential inaccuracies in their responses, the author provided participants with background information to contextualize the study. While this lack of familiarity took some participants outside their comfort zone, it ultimately contributed to valuable insights for the research analysis.

Finally, time and resource constraints posed limitations to this study. The scope of this study was deliberately defined to align with the timeframe allocated for a PhD project, ensuring that the research remained feasible and manageable. Focusing the empirical work within these parameters allowed for a thorough investigation into holistic dark data governance while maintaining the necessary depth and rigor. While additional time could have facilitated a more expansive Delphi process or extended the study to include multiple universities, the chosen scope enabled the research to deliver meaningful insights within the available resources. By concentrating efforts on a focused context, the study establishes a solid foundation for future research in holistic dark data governance, offering valuable contributions to the field and creating opportunities for broader exploration in subsequent work.

8.5. Recommendations for Future Research

Holistic dark data governance is an emerging field, and this research represents a foundational contribution to future inquiry. Several key areas for further investigation have been identified and merit academic exploration:

1. Future research could focus on the practical implementation of a holistic dark data governance system, based on the proposed model. This would require identifying and managing primary business functions alongside dark data governance support functions within the VSM context.
2. Conducting empirical studies on holistic dark data governance in different countries to facilitate comparative analysis and the adoption of international best practices.
3. Leveraging the findings of this thesis to contribute to the development of new dark data governance standards that can be implemented across organisations and made auditable.
4. Developing Metrics and key performance indicators (KPIs) for Holistic Dark Data Governance. Future research could focus on identifying KPIs and metrics to assess the efficiency of the dark data governance model. These metrics could be applied across industries to standardize the measurement of holistic dark data governance performance, maturity, and outcomes.
5. Expanding the research to examine additional levels of the organisational Viable System Model (VSM) could yield a deeper understanding of the interactions between governance layers, thereby enhancing the development of more robust and scalable governance models. Such an extension would not only contribute to the theoretical foundation of holistic dark data governance but also offer valuable practical insights for organisations seeking to implement governance systemic functions across multiple levels of their global operations.
6. Each phase of the holistic model developed in this thesis could form the basis of standalone research projects, allowing for in-depth exploration—such as studying dark data governance about systemic function interactions.
7. Exploring the ethical dimensions of holistic dark data governance is a critical area for future research. This could involve investigating privacy implications, data ownership challenges, and compliance with relevant international data protection regulations.
8. The convergence of governance domains such as IT governance, corporate governance, and AI governance with data governance is an area of growing academic interest. While convergence presents considerable potential, it also introduces challenges, particularly concerning privacy, security, and governance. The absence of mature governance standards

for converged environments opens substantial opportunities for further research, particularly in addressing dark data governance within a holistic framework that encompasses all relevant governance domains within organisations.

9. Investigating the integration of dark data governance with external organisations, establishing it as a standard requirement for managing data sourced from external environments.
10. Expanding the validation of this thesis' findings across the entire educational sector in the USA, as well as extending the analysis to other sectors and industries.
11. Exploring the integration of the findings from this research within the framework of the USA's digital transformation vision, both in the educational sector and other industries.
12. Examining how AI-powered tools and techniques can be incorporated into holistic dark data governance models to enhance automation, predictive analytics capabilities, and overall decision-making processes related to the identification, classification, and management of dark data assets
13. Developing an automated tool for the assessment and implementation of dark data governance initiatives, tailored to organisational requirements, presents significant potential value.

References

- Abraham, R., Schneider, J. and Brocke, v, J. (2019) "Data governance: A conceptual framework, structured review, and research agenda," , 49,p. 424-438. Available at: <https://doi.org/10.1016/j.ijinfomgt.2019.07.008>.
- Abu-Tapanjeh, M, A. (2009) "Corporate governance from the Islamic perspective: A comparative analysis with OECD principles," , 20(5),p. 556–567. Available at: <https://doi.org/10.1016/j.cpa.2007.12.004>.
- Acero, R, Á., Gonzales, A. and Raymundo, C. (2019) "Data governance reference model under the lean methodology for the implementation of successful initiatives in the peruvian microfinance sector," ,p. 1–11. Available at: <https://doi.org/10.1145/3328833.3328859>.
- Achterbergh, J. and Vriens, D. (2002) "Managing viable knowledge," , 19,p. 223–241. .
- Achterbergh, J. and Vriens, D. (2002) "Managing viable knowledge," , 19,p. 223–241. Available at: IHFPk9EjrOjt4KL9UBCY.
- Adler, M. and Ziglio, E. (1996) "Gazing into the oracle: The Delphi method and its application to social and public health," Jessica Kingsley. .
- Adler, S. (2007) The IBM data governance council maturity model: Building a roadmap for effective data governance. Available at: https://www-935.ibm.com/services/uk/cio/pdf/leverage_wp_data_gov_council_maturity_model.pdf.
- Agarwal, M. (2021) Top 3 challenges for data & analytics leaders. Available at: <https://www.kdnuggets.com/2021/04/top-3-challenges-data-analytics-leaders.html>.
- Agrawal, S. (2019) CIOs can harness dark data to boost innovation. .
- Ajis, M, F, A. and Baharin, H, S. (2019) "Dark data management as frontier of information governance," ,p. 1–5. Available at: <https://doi.org/10.1109/iscaie.2019.8743915>.
- Al-Ruithe, M. (2018) Development and evaluation of a holistic framework and maturity assessment tools for data governance in cloud computing environments. Available at: <http://eprints.staffs.ac.uk/4331/>.
- Al-Ruithe, M. and Benkhelifa, E. (2017) "Analysis and classification of barriers and critical success factors for implementing a cloud data governance strategy," ,p. 467–474. .
- Al-Ruithe, M., Benkhelifa, E. and Hameed, K. (2018) "Data Governance Taxonomy: Cloud versus Non-Cloud," Multidisciplinary Digital Publishing Institute, 10(1),p. 95-95. Available at: <https://doi.org/10.3390/su10010095>.
- AlGhamdi, S., Win, T, K. and Vlahu-Gjorgievska, E. (2020) "Information security governance challenges and critical success factors: Systematic review," , 99,p. 102030-102030. Available at: <https://doi.org/10.1016/j.cose.2020.102030>.
- Alreemy, Z. et al. (2016) "Critical success factors (CSFs) for information technology governance (ITG)," , 36(6),p. 1–8. Available at: <https://doi.org/10.1016/j.ijinfomgt.2016.05.017>.
- Amberg, M., Fischl, F. and Wiener, M. (2005) Background of critical success factor research. Available at: http://www.international-outsourcing.de/CSF-Tool/docs/WorkingPaper_BackgroundCSF_Ambergetal._FINAL.pdf.
- Amitech. (2022) Data governance. Available at: <https://amitechsolutions.com/moderndata-management/data-governance/>.
- Anderton, R. (1989) "The Viable System Model: Interpretations and Applications - The need for formal development of the VSM," John Wiley & Sons,p. 39–50. .
- Andrew, A. (2007) "Organisations as complex systems: An introduction to knowledge cybernetics," , 36,p. 822–824. Available at: <https://doi.org/https://doi.org/10.1108/03684920710749875>.

- Arghand, A, A. (2022) "Viable IT risk management system by viable system model (VSM): Action research for managing IT-related risk in the banking service," 35(6), p. 747-763. Available at: <https://doi.org/10.1007/s11213-021-09587-4>.
- Argyris, C. and Schön, A, D. (1978) "Organisational learning: A theory of action perspective," p. 345-345. Available at: <https://doi.org/10.2307/40183951>.
- Arisandi, D. and Khudri, Y, M, T. (2021) "Analysis and design of data governance at the financial services authority," 17(1), p. 1–6. Available at: <https://doi.org/10.21107/infestasi.v17i1.10515>.
- Ashby, R, W. (1956) An introduction to cybernetics. Available at: <https://doi.org/10.5962/bhl.title.5851>.
- Baguley, I. et al. (2014) "Paroxysmal sympathetic hyperactivity after acquired brain injury: Consensus on conceptual definition, nomenclature, and diagnostic criteria," 31(17), p. 1515-1520. Available at: <https://doi.org/10.1089/neu.2013.3301>.
- Baker, S., Edwards, R. and Doidge, M. (2012) How many qualitative interviews is enough? Expert voices and early career reflections on sampling and cases in qualitative research. Available at: https://cris.brighton.ac.uk/ws/files/301922/how_many_interviews.pdf.
- Bargagliotti, E, A. et al. (2020) "Undergraduate learning outcomes for achieving data acumen," 28(2), p. 197-211. Available at: <https://doi.org/10.1080/10691898.2020.1776653>.
- Barnes, E. et al. (2012) "Development of the maturity matrix dentistry (MMD): A primary care dental team development tool," 212(12), p. 583–587. Available at: <http://www.nature.com/doifinder/10.1038/sj.bdj.2012.523>.
- Başkarada, S., Gao, J. and Koronios, A. (2006) "Agile maturity model approach to assessing and enhancing the quality of asset information in engineering asset management information systems," p. 1–8. Available at: <https://subs.emis.de/LNI/Proceedings/Proceedings85/GI-Proceedings-85-40.pdf>.
- Bauer, M, J. (2005) "Internet governance: Theory and first principles," p. 1–20. Available at: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.113.519&rep=rep1&type=pdf>.
- Becker, J., Knackstedt, R. and Pöppelbuß, J. (2009) "Developing maturity models for IT management," 1(3), p. 213–222. Available at: <https://doi.org/10.1007/s12599-009-0044-5>.
- Beecham, S. et al. (2005) "Using an expert panel to validate a requirements process improvement model," 76(3), p. 251–275. Available at: <https://doi.org/10.1016/j.jss.2004.06.004>.
- Beer, S. (1959) "Cybernetics and management," The English Universities Press. .
- Beer, S. (1967) "Management science: The business use of operations research," Aldus Books.
- Beer, S. (1972) "Brain of the firm," Allen Lane. .
- Beer, S. (1979) "The heart of enterprise," John Wiley & Sons. .
- Beer, S. (1979) "The heart of enterprise," John Wiley & Sons. Available at: [7i4pzyLi7YAiZFHfCnmG](https://doi.org/10.1016/j.jss.2004.06.004).
- Beer, S. (1981) "Brain of the firm, 2nd Edition," John Wiley. .
- Beer, S. (1981) "Brain of the firm, 2nd Edition," John Wiley. Available at: [c993aETsuzvCsUSHlzn](https://doi.org/10.1016/j.jss.2004.06.004).
- Beer, S. (1984) "The viable system model: Its provenance, development, methodology, and pathology," 35, p. 7–25. .
- Beer, S. (1985) "Diagnosing the system for organisations," John Wiley & Sons. .
- Beer, S. (1985) "Diagnosing the system for organisations," John Wiley & Sons. .
- Beer, S. (1985) "Diagnosing the system for organisations," John Wiley & Sons. Available at: [t36KC51t1ELPBfFJqPvS](https://doi.org/10.1016/j.jss.2004.06.004).

- Bell, E. T. and Esch, K. (2016) "The space shuttle: A case of subjective engineering," , 26(6),p. 42-46. Available at: <https://doi.org/10.1109/6.29339>.
- Benfeldt, O. (2017) "A comprehensive review of data governance literature," ,p. 120-133. Available at: <https://aisel.aisnet.org/iris2017/3/>.
- Bijl, R. (1992) "Delphi in a future scenario study on mental health and mental health care," , 24(3),p. 232–250. Available at: [https://doi.org/10.1016/0016-3287\(92\)90033-c](https://doi.org/10.1016/0016-3287(92)90033-c).
- Blommerde, T. and Lynch, P. (2016) "A maturity matrix for assessing service innovation capability," ,p. 1–27. .
- Blommerde, T. and Lynch, P. (2016) "A maturity matrix for assessing service innovation capability," ,p. 1–27. .
- Boehm, B. and Valerdi, R. (2008) "Achievements and challenges in COCOMO-Based software resource estimation," , 25(5),p. 74–83. Available at: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4602679>.
- Borgman, P. H. et al. (2016) "Dotting the I and crossing (out) the T in IT governance: New challenges for information governance," ,p. 1–15. Available at: <https://doi.org/10.1109/hicss.2016.608>.
- Borne, K. (2014) Top 5 big data governance issues. .
- Borrego, M., Douglas, P. E. and Amelink, C. (2009) "Quantitative, qualitative, and mixed research methods in engineering education," , 98(1),p. 53–66. Available at: <https://doi.org/10.1002/j.2168-9830.2009.tb01005.x>.
- Brent, E. and Leedy, D. P. (2010) "Practical research: Planning and design," , 18(2),p. 248-248. Available at: <https://doi.org/10.2307/1318509>.
- Brocklesby, J., Cummings, S. and Davies, J. (1995) "Demystifying the viable systems model as a tool for organisational analysis," , 12,p. 65–86. Available at: AkTHM5oxTUvaYoRzfAaX.
- Brous, P., Janssen, M. and Vilminko-Heikkinen, R. (2016) "Coordinating decision-making in data management activities: A systematic review of data governance principles," ,p. 115–126. Available at: https://link.springer.com/chapter/10.1007/978-3-319-44421-5_9#citeas.
- Bruck, C. (2017) Challenges and opportunities of Data Governance in private and public organisations. .
- Bruin, D. R. and Solms, v, S. (2015) "Modelling cyber security governance maturity," ,p. 1–10. Available at: <https://doi.org/10.1109/istas.2015.7439415>.
- Bruin, D. R. and Solms, v, S. (2016) Cybersecurity Governance: How can we measure it?. Available at: <https://doi.org/10.1109/istafrica.2016.7530578>.
- Bruin, d, T. et al. (2005) "Understanding the main phases of developing a maturity assessment model," ,p. 1–10. Available at: https://www.researchgate.net/profile/Michael_Rosemann2/publication/27482282_Understanding_the_Main_Phases_of_Developing_a_Maturity_Assessment_Model/links/00b7d51f71c388cc54000000.pdf.
- Budgen, D. et al. (2018) "Reporting systematic reviews: Some lessons from a tertiary study," , 95,p. 62–74. Available at: <https://www.sciencedirect.com/science/article/pii/S0950584916303548>.
- Burton, L. (2002) "Methodology and methods in mathematics education research: Where is "The Why"?", ,p. 1–10. .
- Cadavid, H., Andrikopoulos, V. and Avgeriou, P. (2020) "Architecting systems of systems: A tertiary study," , Volume, p. Page numbers. Available at: <https://doi.org/10.1016/j.infsof.2019.106202>.
- Cafarella, M. et al. (2016) "Dark Data: Are we solving the right problems?," ,p. 1–6. Available at: <https://doi.org/10.1145/2882903.2912572>.

- Caldas, M. (2009) "Research design: Qualitative, quantitative, and mixed methods approaches," , 7(1),p. 223-223. Available at: <https://doi.org/10.1590/s1415-65552003000100015>.
- Caralli, A. R., Knight, M. and Montgomery, H, A. (2012) Maturity models 101: A primer for applying maturity models to smart grid security, resilience, and interoperability. Available at: http://resources.sei.cmu.edu/asset_files/WhitePaper/2012_019_001_58920.pdf.
- Cheng, G. et al. (2017) "Cloud data governance maturity model," ,p. 94–99. Available at: <https://doi.org/10.1109/icsess.2017.8342968>.
- Cheng, S. (2018) The Challenge of Dark Data-Experts with impact in information governance. Available at: <https://www.fticonsulting.com/insights/case-studies/challenge-of-dark-data>.
- Cheong, K, L. and Chang, V. (2007) The need for data governance: A case study. Available at: <https://aisel.aisnet.org/acis2007/100/>.
- Clough, P. and Nutbrown, C. (2002) "A student's guide to methodology: justifying enquiry," SAGE Publications. .
- Collibra. (2020) What is data governance and why does it matter?. Available at: <https://www.collibra.com/blog/what-is-data-governance>.
- Correia, J. (2015) Data governance: 5 common pitfalls and how to avoid them. Available at: <https://www.daymarksi.com/information-technology-navigator-blog/data-governance-5-pitfalls-and-how-to-avoid-them>.
- Côrte-Real, N., Ruivo, P. and Oliveira, T. (2020) "Leveraging internet of things and big data analytics initiatives in European and American firms: Is data quality a way to extract business value?", 57(1), p. 103141. Available at: <https://doi.org/10.1016/j.im.2019.01.003>.
- Cousin, G. (2009) Researching learning in higher education: An introduction to contemporary methods and approaches. Available at: <https://ci.nii.ac.jp/ncid/BA8933281X>.
- Crotty, M. (1998) The foundations of social research: Meaning and perspective in the research process. Available at: <https://www.goodreads.com/work/editions/1462103-foundations-of-social-research-meaning-and-perspective-in-the-research>.
- Crowston, K. and Qin, J. (2010) "A capability maturity model for scientific data management," American Society for Information Science and Technology, 1,p. 1–10. .
- Cruzes, S, D. and Dybå, T. (2011) "Research synthesis in software engineering: A tertiary study," , 53(5), p. 440–455. Available at: <https://www.sciencedirect.com/science/article/pii/S095058491100005X>.
- Curry, E., Hasan, S. and Donnellan, B. (2018) "Data governance in smart sustainable cities: The need for proactive dark data governance," , 23,p. 159–175. .
- Curtiss, J., Saxena, S. and Seth, A. (2018) "Transforming data into action: The business outlook for data governance," ,p. 1–10. .
- Dahlberg, T. and Nokkala, T. (2015) "A framework for the corporate governance of data: Theoretical background and empirical evidence," , 13(1),p. 25–45. Available at: <http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=108616811&site=b si-live>.
- Dahlberg, T. and Nokkala, T. (2015) "Corporate governance effect on IT governance in achieving corporate performance," , 6,p. 35–46. .
- Dalkey, C, N. and Helmer, O. (1962) "An experimental application of the Delphi method to the use of experts," , 9(3),p. 458-467. Available at: <https://doi.org/10.1287/mnsc.9.3.458>.
- DAMA. (2017) "The DAMA guide to the data management body of knowledge," Technics Publications. .

- Davies, J. (2002) "Models of governance - a viable systems perspective," , 9(2). Available at: <https://doi.org/10.3127/ajis.v9i2.192>.
- Davies, J. (2002) "Models of governance – a viable systems perspective," , 9,p. 57–66. .
- Davis, D. F. (1989) "Perceived usefulness, perceived ease of use, and user acceptance of information technology," , 13(3),p. 319–340. Available at: <http://www.jstor.org/stable/249008>.
- Davis, R. J. (2011) "Information governance as a holistic approach to managing and leveraging information," , 31. .
- Debreceeny, R. and Gray, L. G. (2013) "IT governance and process maturity: A multinational field study," , 27(1),p. 157–188. Available at: <http://ezproxy.library.capella.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=88181971&site=ehost-live&scope=site>.
- Delbecq, L. A., Ven, d, V, H, A. and Gustafson, H. D. (1976) "Group techniques for program planning: A guide to nominal group and Delphi processes," , 12(4),p. 581-581. Available at: <https://doi.org/10.1177/002188637601200414>.
- Deloitte, P. U. (2017) Dark analytics: Illuminating opportunities hidden within unstructured data: Tech Trends 2017. Available at: <https://dupress.deloitte.com/dup-us-en/focus/tech-trends/2017/dark-data-analyzing-unstructured-data.html>.
- DeNardis, L. (2010) The emerging field of internet governance. Available at: <https://doi.org/10.1093/oxfordhb/9780199589074.013.0026>.
- DGI. (2024) Data governance framework. Available at: <https://datagovernance.com/the-dgi-data-governance-framework/>.
- Donohoe, H., Stelfox, M. and Tennant, B. (2012) Advantages and limitations of the e-Delphi technique: Implications for health education researchers. .
- Dowse, A. and Lewis, E. (2009) "Applying organisational theories to realize adaptive IT governance and service management," ,p. 313-332. Available at: <https://doi.org/10.4018/978-1-60566-008-0.ch018>.
- Dunsin, D. et al. (2023) A Comprehensive Analysis of the Role of Artificial Intelligence and Machine Learning in Modern Digital Forensics and Incident Response. Available at: <https://doi.org/10.2139/ssrn.4554035>.
- Eckerson, W. W. (2017) The rise of augmented analytics: The next wave of disruption in data analytics. .
- Espejo, R. and Gill, A. (2011) The viable system model as a framework for understanding organisations. .
- Espejo, R. and Gill, A. (2011) The viable system model as a framework for understanding organisations. Available at: http://library.uniteddiversity.coop/Systems_and_Networks/Viable_Systems_Model/Viable%20Systems%20Model%20overview.pdf.
- Espejo, R. and Harnden, R. (1989) "The Viable System Model: Interpretations and Applications - The need for formal development of the VSM," John Wiley & Sons,p. 39–50. .
- Espejo, R. and Harnden, R. (1989) "The VSM revisited," ,p. 77–100. .
- Espejo, R. and Reyes, A. (2011) "Organisational systems: Managing complexity with the viable system model," Springer. .
- Espejo, R. and Reyes, A. (2011) "Organisational systems: Managing complexity with the viable system model," Springer. .
- Espejo, R., Bowling, D. and Hoverstadt, P. (1999) "The viable system model and the viplan software," , 28,p. 661–678. .

- Everett, D. (2019) Data governance vs. Data management: What's the difference. Available at: <https://www.informatica.com/blogs/data-governance-vs-data-management-whats-the-difference.html>.
- Fath-Allah, A. et al. (2014) "E-government maturity models: A comparative study," , 5(3),p. 71–91. Available at: <https://ictlogy.net/bibliography/reports/projects.php?idp=2822>.
- Flick, U. (2010) "An introduction to qualitative research," SAGE Publications. .
- Flood, L, R. and Jackson, C, M. (1991) "Creative problem solving," Wiley. .
- Forster, N. and Rockart, J. (1989) "Critical success factors: An annotated bibliography," , 191,p. 3041–3089. .
- Fox, J., Murray, C. and Warm, A. (2003) "Conducting research using web-based questionnaires: practical, methodological, and ethical considerations," , 6(2),p. 167–180. Available at: <https://doi.org/10.1080/13645570210142883>.
- Frick, N. (2012) "Identification of design elements for a maturity model for interorganisational integration: A comparative analysis," ,p. 185–196. Available at: papers3://publication/uuid/3E9C1488-A4E1-44FC-AB0F-99AD7DEE746E.
- Gaertner, J., Green, P. and Heales, J. (2012) "On IT governance structures and their effectiveness in collaborative organisational structures," , 13(3),p. 199–220. Available at: <https://doi.org/10.1016/j.accinf.2012.06.006>.
- Galán, , A. et al. (2017) "Maturity matrix assessment: Evaluation of energy efficiency strategies in brussels historic residential stock," , 111,p. 407–416. Available at: <http://dx.doi.org/10.1016/j.egypro.2017.03.202>.
- Gale, N. et al. (2013) "Using the framework method for the analysis of qualitative data in multi-disciplinary health research," , 13(1). Available at: <https://doi.org/10.1186/1471-2288-13-117>.
- Gallaher, W, D. et al. (2015) "The process of bringing dark data to light: The rescue of the early Nimbus satellite data," , 6,p. 124-134. Available at: <https://doi.org/10.1016/j.grj.2015.02.013>.
- Gartner. (2020) IT glossary: Dark data. Available at: <https://www.gartner.com/it-glossary/dark-data>.
- Gartner. (2020) The state of data governance and management in 2020. .
- Gelbstein, E. (2017) IS audit basics: Data management body of Knowledge—A summary for auditors. Available at: <https://www.isaca.org/resources/isaca-journal/issues/2017/volume-3/is-audit-basics-data-management-body-of-knowledge-a-summary-for-auditors>.
- Geus, d, A. (1999) "The living company: Growth, learning and longevity in business," , 48(7). Available at: <https://doi.org/10.1108/ws.1999.07948gae.003>.
- Gheorghe, M. (2011) "Risk management in IT governance framework," , 14(2),p. 545–552. Available at: <http://www.management.ase.ro/reveconomia/2011-2/27.pdf>.
- Giannarou, L. and Zervas, E. (2014) "Using Delphi technique to build consensus in practice," , 9(2),p. 66–82. Available at: https://www.business-and-management.org/library/2014/9_2--65-82-Giannarou,Zervas.pdf.
- Gimpel, G. (2020) "Bringing dark data into the light: Illuminating existing IoT data lost within your organisation," , 63(4),p. 519-530. Available at: <https://doi.org/10.1016/j.bushor.2020.03.009>.
- Gokhale, B, G. and Banks, D. (2004) "Organisational information security: A viable system perspective," ,p. 178-184. Available at: <https://dblp.uni-trier.de/db/conf/aism/aism2004.html#GokhaleB04>.
- Golkar, A. and Crawley, F, E. (2014) "A framework for space systems architecture under stakeholder objectives ambiguity," , 17(4),p. 479–502. Available at: <https://doi.org/10.1111/sys.21286>.

- Gregory, A. (2011) "Data governance — Protecting and unleashing the value of your customer data assets," Springer Science+Business Media, 12(3),p. 230-248. Available at: <https://doi.org/10.1057/dddmp.2010.41>.
- Guetat, A, B, S. and Dakhli, D, B, S. (2015) "The architecture facet of information governance: The case of urbanized information systems," , 64,p. 1–8. Available at: <https://doi.org/10.1016/j.procs.2015.08.564>.
- Guides, L, U. (2021) Organizing your social sciences research paper. Available at: <https://libguides.usc.edu/writingguide/tiertiarysources>.
- Haes, D, S. and Grembergen, V, W. (2015) "Enterprise governance of information technology," Springer. .
- Hagmann, J. (2013) Information governance - beyond the buzz. .
- Hamel, F. and Herz, T. (2013) "IT evaluation in business groups: A maturity model," ,p. 1410–1417. Available at: <http://dl.acm.org/citation.cfm?id=2480627>.
- Hand, D. (2020) David hand on dark data. Available at: <https://press.princeton.edu/ideas/david-hand-on-dark-data>.
- Hand, J, D. (2020) "Dark data: Why what you don't know matters," Princeton University Press.
- Hasson, F., Keeney, S. and McKenna, H. (2000) "Research guidelines for the Delphi survey technique," , 32(4),p. 1008–1015. Available at: <https://doi.org/10.1046/j.1365-2648.2000.t01-1-01567.x>.
- Heidorn, B, P. (2008) "Shedding light on the dark data in the long tail of science," , 57(2),p. 280–299. Available at: <https://doi.org/10.1353/lib.0.0036>.
- Hert, D, P. and Papakonstantinou, V. (2013) "Three scenarios for international governance of data privacy: Towards an international data privacy organisation, preferably a UN agency?," , 9,p. 272–324. .
- Hevner, R, A. et al. (2004) "Design science in information systems research," , 28(1),p. 75–105. Available at: <http://community.mis.temple.edu/seminars/files/2009/10/hevner-et-al-misq-2004.pdf>.
- Heylighen, F. and Joslyn, C. (2003) "Cybernetics and second-order cybernetics," ,p. 155–170. Available at: <https://doi.org/10.1016/b0-12-227410-5/00161-7>.
- Heylighen, F. and Joslyn, C. (2003) Cybernetics and second-order cybernetics. .
- Hildbrand, S. and Bodhanya, S. (2015) "Guidance on applying the viable system model," , 44,p. 186–201. .
- Hinkle, O. (2020) Three ways organisations can achieve data governance success. .
- HNU. (2020) Data governance maturity model. Available at: <https://hnu.edu/wp-content/uploads/2020/03/Data-Governance-Maturity-Model.pdf>.
- Hsu, C. and Sandford, A, B. (2007) "The Delphi technique: making sense of consensus," , 12(10),p. 1–8. Available at: <http://www.psycholosphere.com/The%20Delphi%20Technique%20-%20Making%20Sense%20of%20Consensus%20by%20Hsu%20&%20Sandford.pdf>.
- Hu, H. and Yan, H. (2013) Modelling of scientific research information management system based on workflow. Available at: <https://doi.org/10.1109/mec.2013.6885121>.
- Huang, K., Lee, W, Y. and Wang, Y, R. (1999) "Quality information and knowledge," ,p. 209–209. Available at: <https://dl.acm.org/citation.cfm?id=288780>.
- Hubbard, D., Freda, A. and Swanagan, A. (2020) "Data Governance 101: IR's Critical Role in Data Governance," Wiley, 2020(185-186),p. 51-65. Available at: <https://doi.org/10.1002/ir.20329>.
- Hummel, M. (2014) "State-of-the-art: A systematic literature review on agile information systems development," ,p. ““. Available at: <https://doi.org/10.1109/hicss.2014.579>.

- Huygh, T. and Haes, D, S. (2018) Using the viable system model to study IT governance dynamics: Evidence from a single case study. Available at: <https://scholarspace.manoa.hawaii.edu/handle/10125/50501>.
- Huygh, T. and Haes, D, S. (2019) "Investigating IT governance through the viable system model," , 36(2),p. 168–192. Available at: <https://doi.org/10.1080/10580530.2019.1589672>.
- IDC. (2018) Worldwide big data and business analytics market forecast. .
- Imtiaz, S. et al. (2013) "A tertiary study: Experiences of conducting systematic literature reviews in software engineering," ,p. 243–248. Available at: <https://doi.org/10.1145/2460999.2461025>.
- ISO/IEC. (2008) "ISO/IEC standard 38500: Corporate governance of information technology," ISO/IEC. .
- ITGI. (2003) Board briefing on IT governance, 2nd edition. Available at: <http://www.itgi.org>.
- ITGI. (2005) Governance of the extended enterprise: Bridging business and IT strategies. Available at: [HxphuRTM40N8rkZzK3v2](http://www.itgi.org/publications/2005/05/governance-of-the-extended-enterprise).
- J., E, J., Linstone, A, H. and Turoff, M. (2002) "The Delphi method: Techniques and applications," , 18(3),p. 363-363. Available at: <https://doi.org/10.2307/1268751>.
- Jackson, C, M. (2003) Systems thinking: Creative holism for managers. Available at: [w9DKNzUbITvfnO9H8dcl](http://www.amazon.com/dp/0974718422).
- Jackson, M. (1991) Systems methodology for the management sciences. Available at: <https://doi.org/10.1007/978-1-4899-2632-6>.
- Jackson, M. (2003) "Systems thinking: Creative holism for managers," Wiley. .
- Jagadish, H. (2022) "Data management and dark data: New challenges and opportunities," , 65,p. 30–32. .
- Janesick, J, V. (2011) "Stretching" exercises for qualitative researchers. .
- Janssen, J. et al. (2013) "Experts' views on digital competence: Commonalities and differences," , 68,p. 473–481. Available at: <https://doi.org/10.1016/j.compedu.2013.06.008>.
- Jim, K, C. and Chang, H. (2018) "The current state of data governance in higher education," , 55(1),p. 198-206. Available at: <https://doi.org/10.1002/pra2.2018.14505501022>.
- Jones, K. et al. (2020) Toward the Development of Data Governance Standards for Using Clinical Free-Text Data in Health Research: Position Paper. Available at: [>>](https://doi.org/10.1111/j.1471-1842.2009.00848.x).
- Judah, S. and White, A. (2021) Hype cycle for data and analytics governance and master data management. .
- Kache, F. and Seuring, S. (2017) "Challenges and opportunities of digital information at the intersection of Big Data Analytics and supply chain management," Emerald Publishing Limited, 37(1),p. 10-36. Available at: <https://doi.org/10.1108/ijopm-02-2015-0078>.
- Karande, A. et al. (2019) "Importance of dark data and its applications," ,p. 1–6. Available at: <https://doi.org/10.1109/icscan.2019.8878776>.
- Keeney, S., Hasson, F. and McKenna, H. (2001) "A critical review of the Delphi technique as a research methodology for nursing," , 38(2),p. 195–200. Available at: [https://doi.org/10.1016/s0020-7489\(00\)00044-4](https://doi.org/10.1016/s0020-7489(00)00044-4).
- Keil, M., Lee, K, H. and Deng, T. (2013) "Understanding the most critical skills for managing IT projects: A Delphi study of IT project managers," , 50(7),p. 398–414. Available at: <https://doi.org/10.1016/j.im.2013.05.005>.
- Kennedy, W. (2005) "Verification and validation of scientific and economic models," ,p. 1–15. .
- Khatri, V. and Brown, C. (2010) "Designing data governance," , 53(1),p. 148-152. Available at: <https://doi.org/10.1145/1629175.1629210>.

- Kim, H. D. (2024) Understanding Systems. Available at: <https://thesystemsthinker.com/introduction-to-systems-thinking/>.
- Kim, W. et al. (2003) A taxonomy of dirty data. .
- Kitchenham, B. and Charters, S. (2007) "Guidelines for performing systematic literature reviews in software engineering," , 2,p. 1051. .
- Kooper, M., Maes, R. and Lindgreen, R. E. (2011) "On the governance of information: Introducing a new concept of governance to support the management of information," , 31(1),p. 195–200. Available at: <https://doi.org/10.1016/j.ijinfomgt.2010.10.007>.
- Kosow, H. and Gassner, R. (2008) "Methods of Future and Scenario Analysis: Overview, assessment, and selection criteria," , 39. Available at: <https://ideas.repec.org/b/zbw/diestu/39.html>.
- Ladley, J. (2012) "Data governance program," Elsevier Inc.. .
- Ladley, J. (2012) "Data Governance: How to Design, Deploy and Sustain an Effective Data Governance Programme," Elsevier Inc.. .
- Lassl, W. (2019) "The viability of organisations vol. 2 - diagnosing and governing organisations," Springer. .
- Laszlo, A. and Krippner, S. (1998) "Systems theories: Their origins, foundations, and development," , 126,p. 47–74. Available at: [https://doi.org/10.1016/s0166-4115\(98\)80017-4](https://doi.org/10.1016/s0166-4115(98)80017-4).
- Lavalle, S. and Smilde, S. (2021) "The governance of dark data: New frontiers in data management," , 13,p. 1–16. .
- Lee, W, Y. et al. (2002) "AIMQ: a methodology for information quality assessment," , 40(2),p. 133–146. Available at: [https://doi.org/10.1016/s0378-7206\(02\)00043-5](https://doi.org/10.1016/s0378-7206(02)00043-5).
- Leonard, A. (2009) "The viable system model and its application to complex organisations," , 4(4),p. 467–483. Available at: <https://doi.org/10.1007/s11213-009-9126-z>.
- Lewis, E. and Canberra, , U. (2010) The viable governance model: A theoretical model for the corporate governance of IT. Available at: [c1mi7ThQZQu8FDNMNnhY](https://doi.org/10.1016/j.ijinfomgt.2010.10.007).
- Loshin, D. (2010) Operationalizing data governance through data policy management. .
- Lowe, D., Espinosa, A. and Yearworth, M. (2020) "Constitutive rules for guiding the use of the viable system model: Reflections on practice," , 287,p. 1014–1035. Available at: <https://www.sciencedirect.com/science/article/pii/S0377221720304768>.
- Lowe, D., Espinosa, Á. and Yearworth, M. (2020) "Constitutive rules for guiding the use of the viable system model: Reflections on practice," , 287(3),p. 1014–1035. Available at: <https://doi.org/10.1016/j.ejor.2020.05.030>.
- Mahanti, R. (2018) "Data governance implementation: critical success factors," Software Quality Professional, 2018, 20(4),p. 4-21. Available at: https://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&auth_type=crawler&jrnl=15220540&AN=132742438&h=b1Qe%2F6WxEnTgETd3YST5M3MG4gEh1n%2FfewuU3heoaMiiMvT7Yh4Wo5D1ZJ1iLbMZayYJSa%2BdtMKYJom9wfUAmg%3D%3D&crl=c.
- Mahanti, R. (2021) "Data governance and compliance," Springer. .
- Maier, A., Moultrie, J. and Clarkson, J, P. (2012) "Assessing organisational capabilities: Reviewing and guiding the development of maturity grids," , 59(1),p. 138–159. Available at: https://www.wiso-net.de/document/ECON__687937566.
- Maniezzo, V. and Colorni, A. (1999) "The impact of data quality information on decision making: An exploratory analysis," , 11(5),p. 853–864. Available at: <https://doi.org/10.1109/69.806935>.
- Marsh, S. (2019) Dark data – the blind spots in your analytics. .
- Martínez, F, A. and Largo, L, F. (2009) "An IT governance framework for universities in spain," ,p. 1–13. Available at:

- <https://rua.ua.es/dspace/bitstream/10045/11216/1/EUNIS%202009%20-%20An%20IT%20Governance%20Framework%20for%20Universities%20in%20Spain%20-%20Fernandez%20y%20Llorens.pdf>.
- Marus, P. (2018) Dark data: A complex challenge for enterprises and CIOs in the cloud era - ET CIO. Available at: <https://cio.economictimes.indiatimes.com/news/strategy-and-management/dark-data-a-complex-challenge-for-enterprises-and-cios-in-the-cloud-era/64575418>.
- McNulty, K. (2017) Expanding the definition of dark data and mining it with dark analytics - make light of your data. Available at: <https://www.prowesscorp.com/expanding-the-definition-of-dark-data-and-mining-it-with-dark-analytics/>.
- Meghji, S. (2017) Data is holding back AI. .
- Melnikovas, A. (2018) "Towards an explicit research methodology: Adapting research onion model for futures studies," , 23(2),p. 29–44. Available at: <https://www.airitilibrary.com/Publication/alDetailedMesh?DocID=10276084-201812-201901170001-201901170001-29-44>.
- Mento, A. (2002) A change management process: Grounded in both theory and practice. .
- Mingers, J. and White, L. (2010) "A review of the recent contribution of systems thinking to operational research and management science," , 207(3),p. 1147–1161. Available at: <https://doi.org/10.1016/j.ejor.2009.12.019>.
- Mohammed, A, A. (2023) Gender related issues and ecosystem service utilization within the volta basin: Field level qualitative experiences. Available at: <https://doi.org/10.11648/j.ijaas.20230901.13>.
- Moultrie, J., Sutcliffe, L. and Maier, A. (2016) "A maturity grid assessment tool for environmentally conscious design in the medical device industry," , 122,p. 252–265. Available at: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-84959331528&partnerID=40&md5=a96da8444daf33095e97eb42b28ade56>.
- Mullen, P. (2003) "Delphi: Myths and reality," , 17(1),p. 37–52. Available at: <https://doi.org/10.1108/14777260310469319>.
- Müller, R. and Jugdev, K. (2012) "Critical success factors in projects," , 5(4),p. 757–775. Available at: <https://doi.org/10.1108/17538371211269040>.
- Mulrow, C. and Cook, D. (1998) Systematic reviews: Synthesis of best evidence for health care decisions. .
- Nagle, T. and Sammon, D. (2017) "The data value map: A framework for developing shared understanding on data initiatives," ,p. 1439-1452. Available at: https://cora.ucc.ie/bitstream/10468/5167/1/4404_ECIS_2017_-_The_Data_Value_Map_-_Developing_a_Shared_Understanding_for_Data_Initiatives.pdf.
- Nascio. (2009) "Data governance part II: Maturity models – a path to progress," ,p. 1–30. .
- Niazi, M., Cox, K. and Verner, J. (2007) "A measurement framework for assessing the maturity of requirements engineering process," , 16(2),p. 213–235. Available at: <https://doi.org/10.1007/s11219-007-9033-4>.
- NICCS. (2022) Explore terms: A glossary of common cybersecurity terminology. Available at: https://niccs.us-cert.gov/glossary#letter_c.
- Niemi, E. (2011) Designing a data governance framework. Available at: [https://research.aalto.fi/en/publications/designing-a-data-governance-framework\(7af480e7-f032-48c8-8025-fd26fc4589f9\).html](https://research.aalto.fi/en/publications/designing-a-data-governance-framework(7af480e7-f032-48c8-8025-fd26fc4589f9).html).
- Niemi, E. and Laine, S. (2016) "Designing information governance with a focus on competence management in a knowledge-intensive project organisation," ,p. 1–12. Available at: <https://dblp.uni-trier.de/db/conf/iq/iq2016.html#NiemiL16>.
- Ning, Z. (2016) An overview of data governance. .

- Oberkampff, L. W. and Trucano, T. (2008) "Verification and validation benchmarks," , 238(3),p. 716–743. Available at: <https://doi.org/10.1016/j.nucengdes.2007.02.032>.
- Okoli, C. and Pawlowski, D. S. (2004) "The Delphi method as a research tool: an example, design considerations and applications," , 42(1),p. 15–29. Available at: <https://doi.org/10.1016/j.im.2003.11.002>.
- Olaitan, O., Herselman, M. and Wayi, N. (2016) Taxonomy of literature to justify data governance as a prerequisite for information governance. .
- Omar, A. and Almaghthawi, A. (2020) "Towards an Integrated Model of Data Governance and Integration for the Implementation of Digital Transformation Processes in the Saudi Universities," Science and Information Organisation, 11(8). Available at: <https://doi.org/10.14569/ijacsa.2020.0110873>.
- Otto, B. (2011) "Organizing data governance: findings from the telecommunications industry and consequences for large service providers," , 29,p. 1–9. Available at: <https://doi.org/10.17705/1cais.02903>.
- Otto, B. (2011) A morphology of the organisation of data governance. Available at: <https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1271&context=ecis2011>.
- Overby, E., Bharadwaj, A. and Sambamurthy, V. (2006) "Enterprise agility and the enabling role of information technology," , 15(2),p. 120–131. Available at: <https://doi.org/10.1057/palgrave.ejis.3000600>.
- Owuonda, S. and Orwa, D. (2016) "Cloud computing governance readiness assessment: Case study of a local airline company," , 10(8),p. 95. Available at: <http://www.mdpi.com/2071-1050/10/1/95>.
- Patunob, B. G. and Ibojo, M, T, D. (2023) "Best practices in teaching world literature: A phenomenological study," , 19(1),p. 1310-1315. Available at: <https://doi.org/10.30574/wjarr.2023.19.1.1507>.
- Paucar-Caceres, A. and Pagano, R. (2009) "Systems thinking and the use of systemic methodologies in knowledge management," , 26,p. 343–355. .
- Peffers, K. et al. (2007) "A design science research methodology for information systems research," , 24(3),p. 45–77. Available at: <https://doi.org/10.2753/mis0742-1222240302>.
- Peppard, J. (2005) The application of the viable systems model to IT governance. Available at: <http://www.som.cranfield.ac.uk/som/p2102/People/Faculty/Academic-Faculty-Listing-A-Z/Last-Name-P/Joe-Peppard>.
- Permana, I, R. and Suroso, S, J. (2018) "Data governance maturity assessment at PT. XYZ. Case study: Data management division," ,p. 1–5. Available at: <https://doi.org/10.1109/icimtech.2018.8528142>.
- Petersen, K. et al. (2008) "Systematic mapping studies in software engineering," , 17,p. 10. Available at: http://www.cse.chalmers.se/~feldt/publications/petersen_ease08_sysmap_studies_in_se.pdf.
- Peterson, R. (2004) "Integration strategies and tactics for information technology governance," ,p. 37–80. Available at: <https://doi.org/10.4018/9781591401407.ch002>.
- Pinto, K, J. and Prescott, E, J. (1988) "Variations in critical success factors over the stages in the project life cycle," , 14(1),p. 5–18. Available at: <https://doi.org/10.1177/014920638801400102>.
- Pohlman, M. (2010) Using the CSA control matrix and ISO 27017 controls to facilitate regulatory compliance in the cloud. .
- Pollalis, A, Y. and Dimitriou, K, N. (2008) "Knowledge management in virtual enterprises: A systemic multi-methodology towards the strategic use of information," , 28(4),p. 305–321. Available at: <https://doi.org/10.1016/j.ijinfomgt.2008.02.001>.

- Preece, G. (2010) Information management for viable organisation. .
- Preece, G. (2010) Information management for viable organisation. Available at: [VgKd9k1DfWp8wJYVUxfp](http://eprints.aston.ac.uk/16495/1/Information%2Bmanagement%2Bfor%2Bviable%2Borganisations(2011).pdf).
- Preece, G., Shaw, D. and Hayashi, H. (2013) "Using the viable system model (VSM) to structure information processing complexity in disaster response," , 224,p. 209–218. .
- Preece, G., Shaw, D. and Hayashi, H. (2013) "Using the Viable System Model (VSM) to structure information processing complexity in disaster response," , 224,p. 209–218. .
- Preece, G., Shaw, D. and Hayashi, H. (2013) "Using the Viable System Model (VSM) to structure information processing complexity in disaster response," , 224,p. 209–218. .
- Preece, R, G. (2010) Information management for viable organisations. Available at: [http://eprints.aston.ac.uk/16495/1/Information%2Bmanagement%2Bfor%2Bviable%2Borganisations\(2011\).pdf](http://eprints.aston.ac.uk/16495/1/Information%2Bmanagement%2Bfor%2Bviable%2Borganisations(2011).pdf).
- Preittigun, A., Chantatub, W. and Vatanasakdakul, S. (2012) "A comparison between IT governance research and concepts in COBIT 5," , 2(6),p. 581–590. Available at: <https://researchers.mq.edu.au/en/publications/a-comparison-between-it-governance-research-and-concepts-in-cobit>.
- Preston, D. and Karahanna, E. (2009) "Antecedents of IS strategic alignment: A nomological network," , 20(2),p. 159–179. Available at: <https://doi.org/10.1287/isre.1070.0159>.
- Price, R. and Shanks, G. (2004) "A semiotic information quality framework," ,p. 1–11. .
- Prinzo, R. (2012) Developing a strategy for your data governance initiative. Available at: https://hcexchange.conference-board.org/attachment/Rob-Prinzo---WSR_JunJul12_all-3.pdf.
- Provost, J. and Danyluk, A. (1995) "Learning from bad data," ,p. 114–121. .
- Purss, B, M. et al. (2015) "Unlocking the Australian Landsat archive – from dark data to high performance data infrastructures," , 6,p. 272–275. Available at: <https://doi.org/10.1016/j.grj.2015.02.010>.
- Ragab, M. and Arisha, A. (2017) "Research methodology in business: A starter's guide," , 5(1),p. 1-1. Available at: <https://doi.org/10.5430/mos.v5n1p1>.
- Ramírez–Vizcaya, S. and Froese, T. (2019) "The Enactive Approach to Habits: New Concepts for the Cognitive Science of Bad Habits and Addiction," *Frontiers Media*, 10. Available at: <https://doi.org/10.3389/fpsyg.2019.00301>.
- Rau, G, K. (2004) "Effective governance of IT: Design objectives, roles, and relationships," , 21(4),p. 35–42. Available at: <https://doi.org/10.1201/1078/44705.21.4.20040901/84185.4>.
- Ray, M. (2024) Chernobyl disaster. Available at: <https://www.britannica.com/event/Chernobyl-disaster>.
- Redman, C, T. (2018) If your data is bad, your machine learning tools are useless. .
- Redman, T. (2016) Bad data costs the U.S. \$3 trillion per year. Available at: <https://hbr.org/2016/09/bad-data-costs-the-u-s-3-trillion-per-year>.
- Rees, V, I. (2007) The evolution of dark data and how it makes your business smarter. .
- Rees, V, I. (2020) The evolution of dark data and how it makes your business smarter. .
- Reynolds, M. and Holwell, S. (2010) "Systems approaches to managing change: A practical guide," Springer. Available at: <https://doi.org/10.1007/978-1-84882-809-4>.
- Reynolds, M. and Holwell, S. (2010) Systems approaches to managing change: A practical guide. Available at: <https://doi.org/10.1007/978-1-84882-809-4>.
- Rezaee, Z. et al. (2018) "Application of viable system model in diagnosis of organisational structure," , 32(3),p. 273–295. Available at: <https://doi.org/10.1007/s11213-018-9454-y>.
- Richter, J. and Basten, D. (2014) "Applications of the viable systems model in IS research – A comprehensive overview and analysis," ,p. 4589–4598. .

- Rios, P, J. (2012) Design and diagnosis for sustainable organisations. Available at: dJ1RicGwuHJXFtJW0VsL.
- Rivera, E. et al. (2017) "Data governance maturity model for micro financial organisations in peru," ,p. 203–214. Available at: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85023167622&partnerID=40&md5=75dfca25fc7ac9709fbc5c63a5e504ad>.
- Roberts, M, C. (2010) "The dissertation journey," Corwin Press. .
- Rose, J. and Guide, P. (2013) Selecting, using, and creating maturity models: A tool for assurance and consulting engagements. Available at: https://www.iaa.org.uk/media/358857/selecting__using__and__creating_maturity_models_-_a_tool_for_assurance_and_consulting_engagements.pdf.
- Rowe, G. and Wright, G. (1999) "The delphi technique as a forecasting tool: Issues and analysis," , 15(4),p. 353–375. Available at: [https://doi.org/10.1016/s0169-2070\(99\)00018-7](https://doi.org/10.1016/s0169-2070(99)00018-7).
- Ryu, S, K., Park, S, J. and Park, J. (2006) "A data quality management maturity model," , 28(2),p. 191–204. Available at: <http://etrij.etri.re.kr/Cyber/BrowseAbstract.jsp?vol=28&num=2&pg=191>.
- Saidah, S, A. and Abdelbaki, N. (2014) "A new cloud computing governance framework," ,p. 671–678. Available at: <http://www.scopus.com/inward/record.url?eid=2-s2.0-84902352099&partnerID=40&md5=cedce19630e88e4321cd8e9234b59920>.
- Saleh, M. (2011) "Information security maturity model," , 5,p. 316–337. Available at: <http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Information+Security+Maturity+Model#0>.
- Saleh, M. et al. (2008) "A survey on futures studies methods," ,p. 38–46. .
- Sargent, G, R. (2013) "Verification and validation of simulation models," Taylor & Francis, 7(1),p. 12-24. Available at: <https://doi.org/10.1057/jos.2012.20>.
- Sarsfield, S. (2009) "The data governance imperative," ,p. 31–36. Available at: <https://dl.acm.org/citation.cfm?id=1611416>.
- Schembera, B. and Durán, M, J. (2020) "Dark data as the new challenge for big data science and the introduction of the scientific data officer," , 33(1),p. 93–115. Available at: <https://doi.org/10.1007/s13347-019-00346-x>.
- Schipper, J. (2002) The dynamic architecture maturity matrix: Assessment analysis and instrument validation. .
- Schwaninger, M. (1990) "Embodiments of organisational fitness: the viable system model (VSM) as a guide," , 3,p. 249–264. Available at: y6O9wICCOYSzQ2FY0fbY.
- Schwaninger, M. (2006) "Design for viable organisations: The diagnostic power of the viable system model," , 35,p. 955–966. .
- Schwaninger, M. (2018) Governance for intelligent organisations: a cybernetic contribution. .
- Schwaninger, M. and Ríos, J. (2008) "System dynamics and cybernetics: A synergetic pair," , 24,p. 145–174. .
- Shaw, R, D. et al. (2004) "The viable systems model applied to a smart network: the case of the UK electricity market," , 19(4),p. 270–280. .
- Shaw, R, D. et al. (2004) "The viable systems model applied to a smart network: the case of the UK electricity market," , 19(4),p. 270–280. Available at: <https://doi.org/10.1057/palgrave.jit.200002>.
- Silic, M. and Bäck, A. (2013) "Factors impacting information governance in the mobile device dual-use context," , 23(2),p. 73–89. Available at: <http://www.emeraldinsight.com/doi/10.1108/RMJ-11-2012-0033>.
- Simon, M. and Goes, J. (2011) Developing a theoretical framework. Available at: <http://www.dissertationrecipes.com>.

- Skulmoski, J. G., Hartman, T. F. and Krahn, R. J. (2007) "The Delphi method for graduate research," , 6,p. 1–21. Available at: <https://doi.org/10.28945/199>.
- Smallwood, F. R. (2012) "The Onslaught of Big Data and the Information Governance Imperative," ,p. 1-13. Available at: <https://doi.org/10.1002/9781118433829.ch1>.
- Snowflake, D. (2019) 5 steps to successful data governance. .
- Solemon, B. (2013) "Evaluation criteria for requirements engineering process improvement models and frameworks," ,p. 15–20. .
- Sourani, A. and Sohail, M. (2014) "The Delphi Method: Review and Use in Construction Management Research," Taylor & Francis, 11(1),p. 54-76. Available at: <https://doi.org/10.1080/15578771.2014.917132>.
- Splunk. (2019) The state of dark data. Available at: <https://www.splunk.com/pdfs/dark-data/the-state-of-dark-data-report.pdf>.
- Stedman, G. and Vaughan, J. (2020) What is data governance and why does it matter?. Available at: <https://searchdatamanagement.techtarget.com/definition/data-governance>.
- Sun, Z., Su, T. and Shen, Y. (2023) "Dark data in organisations: Risks, governance strategies, and case studies," , 32(3),p. 473-519. Available at: <https://doi.org/10.1111/isj.12355>.
- Sundarraj, M. and Natrajan, M. R. (2019) "A sustainable method to handle dark data in a smart factory," , 21,p. 1–7. Available at: <https://asq.org/software-quality/2019/08/software-quality/a-sustainable-method-to-handle-dark-data-in-a-smart-factory.pdf>.
- Texas-A&M. (2018) Texas A&M. Available at: <https://it.tamus.edu/governance/it-governance-framework/>.
- Thiel, R., Stroetmann, K. and Singleton, P. (2014) "Clinical data governance: legal and ethical challenges," ,p. 1–7. .
- Thomas, G. (2020) In depth: The DGI data governance framework. Available at: <https://datagovernance.com/the-dgi-data-governance-framework/>.
- Trajanov, D. et al. (2018) "Dark data in internet of things (IoT): Challenges and opportunities," ,p. 1–4. Available at: <https://doi.org/10.1109/meco.2018.8406012>.
- UNT. (2024) University of North Texas. Available at: <https://www.unt.edu/index.html>.
- UT@Austin. (2024) Common data set - University of Texas at Austin. Available at: <https://reports.utexas.edu/common-data-set>.
- UTIMCO. (2024) Funds managed by UTIMCO. Available at: <https://www.utimco.org/funds-managed/>.
- Valentine, E. and Stewart, G. (2013) "The emerging role of the Board of Directors in enterprise business technology governance," , 10(2),p. 346–362. Available at: <https://doi.org/10.1057/jdg.2013.14>.
- Veaux, D. D. R. and Hand, J. D. (2005) "How to lie with bad data," , 20(3),p. 231–238. Available at: <https://doi.org/10.1214/088342305000000269>.
- Venable, J., Pries-Heje, J. and Baskerville, R. (2016) "FEDS: A framework for evaluation in design science research," , 25(1),p. 77–89. Available at: <https://doi.org/10.1057/ejis.2014.36>.
- Venkatesh, V., Brown, A. S. and Bala, H. (2013) "Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems," , 37(1),p. 21–54. Available at: <https://doi.org/10.25300/misq/2013/37.1.02>.
- Victor, E. (2016) An assessment of data governance at kenya health professionals regulatory authorities. Available at: <http://erepository.uonbi.ac.ke/handle/11295/98456>.
- Weber, K., Otto, B. and Osterle, H. (2009) "One size does not fit all — A contingency approach to data governance," , 1,p. 4:1–4:27. Available at: <http://dl.acm.org/citation.cfm?id=1515696>.

- Wende, K. (2007) "A model for data governance – organizing accountabilities for data quality management," ,p. 417–425. .
- Wibowo, A, M. and Waluyo, R. (2015) "Knowledge management maturity in construction companies," , 125,p. 89–94. Available at: <http://dx.doi.org/10.1016/j.proeng.2015.11.014>.
- Wibowo, S, N., Utami, E. and Fatta, A, H. (2021) Perancangan Structure Tata Kelola Data di Pemerintah Daerah Menggunakan Framework Data Management Body Of Knowledge. Available at: <http://e-journal.unipma.ac.id/index.php/RESEARCH/article/viewFile/7049/pdf>.
- Wiebe, H, P. and Allison, D, M. (2015) "Bringing dark data into the light: A case study of the recovery of Northwestern Atlantic zooplankton data collected in the 1970s and 1980s," , 6,p. 195-201. Available at: <https://doi.org/10.1016/j.grj.2015.03.001>.
- Wiener, N. (1948) "Cybernetic or control and communication in animal and the machine," John Wiley & Sons. .
- Wiener, N. (1948) Cybernetics: Or the control and communication in the animal and the machine. .
- Williams, B. and Hummelbrunner, R. (2010) "Systems concepts in action: a practitioner's toolkit," Stanford University Press. Available at: [KL16gSYqqYdudKuUa6hh](https://doi.org/10.1162/SYQYDUDKUUA6HH).
- Williams, P. (2007) "Information governance: a model for security in medical practice," , 2,p. 57–74. Available at: <https://doi.org/10.15394/jdfsl.2007.1017>.
- Woldu, L. (2013) Lewam woldu cloud governance model and security solutions for cloud service providers. .
- Xia, Y., Yao, H. and Zhang, M. (2022) "Governance of dark data in the era of big data: A critical review," , 59(8),p. 1–12. Available at: <https://doi.org/10.1016/j.im.2022.103719>.
- Yebenes, J. and Zorrilla, M. (2019) "Towards a data governance framework for third generation platforms," , 160,p. 329–336. Available at: <https://doi.org/10.1016/j.procs.2019.04.082>.
- Yolles, M. (2005) "Organisational intelligence," , 17,p. 99–114. .
- Yolles, M. (2006) "Organisations as complex systems: An introduction to knowledge cybernetics," Information Age Publishing. .
- York, T. (2023) Dark data: Discovery, uses & benefits of hidden data. Available at: https://www.splunk.com/en_us/blog/learn/dark-data.html.
- Yousuf, I, M. (2007) "Using experts' opinions through Delphi technique," , 12,p. 2–8. .
- Yuan, F., Meng, J. and Li, Y. (2020) Research on the Model of “data-based governance” in Colleges and Universities. Available at: <https://doi.org/10.1109/icbdie50010.2020.00012>.
- Yusuwan, M, N. et al. (2021) "Towards a Successful Extension of Time (EoT) Claim: A Consensus View of Construction Professionals via a Modified Delphi Method," Chulalongkorn University, 25(1),p. 263-274. Available at: <https://doi.org/10.4186/ej.2021.25.1.263>.
- Zicari, V, R. (2014) Big data governance and metadata management: Data governance meets big data. Available at: <https://www.zicari.eu>.
- Zolfagharian, M. et al. (2019) "Studying transitions: Past, present, and future," , 48(9),p. 103788. Available at: <https://www.sciencedirect.com/science/article/pii/S0048733319301039>.
- Zolfagharian, M. et al. (2019) Studying transitions: Past, present, and future. .

Appendices

Appendix A: Key Dark Data Types & their Description

Reference: Hand, J. D. (2020)

DD-Type 1: Data We Know Are Missing

These are Rumsfeld's "known unknowns." They arise when we know there are gaps in the data, concealing values that could have been recorded. An example is missing values in a table for certain rows. Related to the source data not gathered – data does not exist in the data source – optional/mandatory data

DD-Type 2: Data We Don't Know Are Missing

These are Rumsfeld's "unknown unknowns." We do not even know that we are missing data. Disasters may arise if decision-makers do not recognize they are missing critical data while finalizing and executing decisions - The data you don't have might make the data you do have of very limited value. Data may exist in the data source but is unknown

DD-Type 3: Choosing Just Some Cases

Poor choice of criteria for data inclusion in a business model, or poor application of reasonable criteria, can lead to the construction of distorted business models. A particular variant arises when some choices based on the distorted model lead to disappointments in the future as regression to the mean kicks in. related to output that misses relevant existing data in the data source

DD-Type 4: Self-Selection

It arises when people themselves can decide whether to be included in a database. Examples: databases for which patients can decide whether to have their data stored (opt-in and opt-out), and more generally in the choice of services that people make (e.g., a bank or supermarket). In all these examples, those included in the database may well differ in some systematic way from those not included. Related to the source data not gathered – data does not exist in the data source – optional data

DD-Type 5: Missing What Matters

Sometimes a critical aspect of a system is entirely unobserved. This can lead to mistaken causal attributions, as when an increase in ice cream sales is followed by grass drying out. Obviously, here the causal network is missing data about the weather—but it's not always so obvious that something is missing. Mixing between Causation vs. correlation

DD-Type 6: Data Which Might Have Been

Counterfactual data are the data we would have seen had we taken some other action or observed what happens under different conditions or circumstances. An example is a clinical trial in which each patient can receive only one treatment—perhaps because the aim of the trial is to investigate the time to cure—so that once a patient has been cured, it is not possible to go back to explore the time the alternative treatment would have taken. Multiple data generation is possible, but one data set can be practically or feasibly collected

DD-Type 7: Changes with Time

Time can hide data in many ways. For example, data might no longer be an accurate description of the current state of the world, cases might not be observed because they occur after the end of the observation period, cases might drop out because they change their nature, and so on. Examples include medical studies of survival times after diagnosis and when the observation period is terminated before a patient has died, and data describing a country's population 20 years ago, which might be of limited value for developing current public policy. Data is time dependent – and can be out of date (ex. Well production rate)

DD-Type 8: Definitions of Data

Definitions might be inconsistent and may change over time to better reflect their purpose and use. This can cause problems with economic (and other kinds of) time series, in which the data underlying them may cease to be collected. More generally, if people define concepts in different ways, they may well draw different conclusions. One example is UK crime statistics, which are measured by police records and by a survey of victims since the two sources have different definitions of a crime. Inconsistent metadata

DD-Type 9: Summaries of Data

By definition, summarizing data means discarding the details. If you report merely an average, you reveal nothing about the range of the data, and nothing about the skewness of the distribution. An average could conceal the fact that some values are very different indeed. Or, at the other extreme, it could conceal the fact that all the values are identical. Derived data may not reflect original data; other derivations are to be made.

DD-Type 10: Measurement Error and Uncertainty

Measurement error leads to uncertainty about the underlying true value. This is most easily seen if we imagine a situation in which the range of measurement error is as large as or larger than the range of underlying true values since then the observed value can be very different from the truth. Rounding, heaping, ceiling, floor effects, and others all inject uncertainty into the data, obscuring precise values. A different cause of uncertainty and inaccuracy is data linkage, in which identifying information might be stored in different styles, making matching error-prone.

DD-Type 11: Feedback and Gaming

This type of data arises when the values of data that have been collected influence the collection process itself— as in grade inflation and share-price bubbles. It means that the data are a distorted representation of the underlying reality—possibly drifting further from it as time progresses.

DD-Type 12: Information Asymmetry

Different data sets may be held by different people, and information asymmetry arises when one knows something that others don't, and one party is able to take advantage of another. Examples are insider trading, Akerlof's market for lemons, and international tensions arising from limited knowledge of an enemy country's capabilities. For example, if a homeowner wanted to sell their house, they would have more information about the house than the buyer. They might know some floorboards are creaky, the home gets too cold in winter, or that the neighbours are too loud; information that the buyer would not know until after they purchased the house. The buyer, then, might feel they paid too much for the house or would not have purchased it at all if they had this information beforehand.

DD-Type 13: Intentionally Darkened Data

This particular example of choosing just some cases is a particularly troublesome one. It arises when people deliberately conceal or manipulate data with intent to deceive or mislead—it is fraud. We saw that it can arise in many contexts and in many ways.

DD-Type 14: Fabricated and Synthetic/Artificial/Fake/manmade Data

When data are made up it might be with the intention to mislead, as in fraud. But it also occurs in simulation, when artificial data sets that could have arisen from the process being studied are generated, and in other applications in which data are replicated, such as bootstrap, boosting, and smoothing. Modern statistical tools make extensive use of such ideas, but poor replication can result in misleading conclusions. Creating artificial sets not in the source data

DD-Type 15: Extrapolating Beyond Your Data

Data sets are necessarily always finite. That means they have a maximum and a minimum value, beyond which lies the unknown. Making statements about possible values above the maximum or below the minimum in a data set requires that assumptions must be made, or that information is acquired from some other source. assuming values not in the original data range

Appendix B: UEL-Approved Ethical Forms

Appendix B.1: Ethical Approval



Dear Fatime Atta

Application ID: ETH2122-0052

Project title: The power of Dark Data - Exploring the Role of Data Governance

Lead researcher: Mrs Fatime Atta Alkhatib

Your application to Ethics and Integrity Sub-Committee was considered on the 7th of December 2021.

The decision is: Approved

The Committee's response is based on the protocol described in the application form and supporting documentation.

Your project has received ethical approval for 4 years from the approval date.

If you have any questions regarding this application, please contact your supervisor or the secretary for the Ethics and Integrity Sub-Committee.

Approval has been given for the submitted application only and the research must be conducted accordingly.

Should you wish to make any changes in connection with this research project you must complete '[An application for approval of an amendment to an existing application](#)'.

The approval of the proposed research applies to the following research site.

Research site: Research will take place through UEL email (No video or audio recording will be required) - It is worth mentioning that Microsoft Teams will be utilized for orientation and clarification purposes not data collection.

Principal Investigator / Local Collaborator: Mrs. Fatime Atta Alkhatib

Approval is given on the understanding that the [UEL Code of Practice for Research and the Code of Practice for Research Ethics](#) is adhered to.

Any adverse events or reactions that occur in connection with this research project should be reported using the University's form for [Reporting an Adverse/Serious Adverse Event/Reaction](#).

The University will periodically audit a random sample of approved applications for ethical approval, to ensure that the research projects are conducted in compliance with the consent given by the Research Ethics Committee and to the highest standards of rigour and integrity.

Please note, it is your responsibility to retain this letter for your records.

With the Committee's best wishes for the success of the project

Yours sincerely

Fernanda Silva

Administrative Officer for Research Governance

B.2 Participant Information Sheet



B.2.1 PARTICIPANT INFORMATION SHEET

University of East London

University Way
London E16 2RD
United Kingdom

Research Integrity

The University adheres to its responsibility to promote and support the highest standard of rigour and integrity in all aspects of research; observing the appropriate ethical, legal and professional frameworks.

The University is committed to preserving your dignity, rights, safety and wellbeing and as such it is a mandatory requirement of the University that formal ethical approval, from the appropriate Research Ethics Committee, is granted before research with human participants or human data commences.

The purpose of this Participant Information Sheet is to provide you with the information that you need to consider in deciding whether to participate in this research project.

The Principal Investigator/Director of Studies

Rabih Bashroush
University Way, London E16 2RD, United Kingdom
r.bashroush@uel.ac.uk

Student researcher

Fatime AlKhatib
University Way, London E16 2RD, United Kingdom
u1829839@uel.ac.uk

B.2.2 PARTICIPANT INFORMATION SHEET



Consent to Participate in a Research Study

The purpose of this letter is to provide you with the information that you need to consider in deciding whether to participate in this Study.

Consent to Participate in a Research Study

The purpose of this letter is to provide you with the information that you need to consider whether to participate in this study.

Project Title

The power of Dark Data* - Exploring the Role of Data Governance**

**Dark data is a general term for the various kinds of bad, missing, unutilized, inconsistent, distorted, or fabricated data*

*** Data Governance: is the exercise of authority and shared decision making (planning, monitoring and enforcement) over the management of data assets*

Project Description

The aim of this study is analysis of current data governance (DG) approaches to manage the power of dark data in organisations. Also, will explore the key dark DG components and core challenges as experienced by data users and other relevant stakeholders. The results of this study will be analysed in conjunction with previous DG work with the goal to explore and conceptualize a holistic novel dark data governance approach at intra-organisational and interorganisational levels with emphasis on continuous improvements. This study is part of an approved PhD research plan and forms the 4th and 5th phases in that plan.

The study will investigate the following key relevant areas:

- Key Data Classes & relevant dark data types within the organisation.
- Key Dark Data Governance Dimensions and Components - for example:
 - o DG Structural Mechanisms: Roles & Responsibilities, Locus of control, etc.
 - o DG Functional Mechanisms: Strategies, policies, standards, processes, issue management, compliance, maturity assessment, change management, etc.
 - o DG Relational Mechanisms: communication, Awareness, training, etc.
 - o DG Domain Scope: Data Quality, Data Security, Data Architecture, Metadata, Data storage, Data integration, data modelling, Content management, Master data, data warehousing & business intelligence, etc.
 - o Data scope: transactional, master, big data, etc.
 - o Contingency factors: industry type, country, Legal& Regulatory Requirements, etc.
- Based on the preceding two steps and existing research and industry knowledge, this research will be conceptualizing a novel dark data governance framework. The conceptualization will be based on a holistic approach taking in consideration the deployment phases (planning,

development, operations, & control) at intra-organisational and inter-organisational levels with emphasis on continuous improvements

- Finally, within the holistic context, this research will conceptualize a data governance maturity model and assessment matrix to ensure a continuous improvement process in managing the different kinds of dark data defined by the organisation

Participants are to provide the relevant feedback data regarding the above relevant areas via email and clarifications can be made as needed (either via email or online)—feedback to be provided by a specified deadline.

Confidentiality of the Data

All data collected during this study will be stored on secured devices (UEL OneDrive) only available to the researcher. Data will be kept for 48 months after which time the primary data will be destroyed. Access to the primary data will be restricted to the researcher and relevant UEL research decision-makers as necessary (personal data will be anonymized). Participants and their associations will not be disclosed and kept strictly confidential unless attribution is specifically permitted. Participants' confidentiality will be maintained unless a disclosure is made that indicates that the participant or someone else is at serious risk of harm. Such disclosures may be reported to the relevant authority. Data generated in the course of the research will be retained in accordance with the University's Data Protection Policy.

In compliance with the General Data Protection Regulation (GDPR) the University's lawful basis for the processing of personal data collected, used, and retained for research purposes is the 'public task' condition. Therefore, the University does not rely on consent to process your personal data. However, the University will seek your consent to participate in this research project. Please see the following link for more information: Data Protection – University of East London (UEL)

Disclaimer

Your participation in this study is voluntary, and you are free to withdraw at any time during the research. Should you choose to withdraw from the programme you may do so without disadvantage to yourself and without an obligation to give a reason. Please note that your data can be withdrawn up to the point of data analysis – after this point, it may not be possible if your data is anonymised.

Ethical Approval for the research project has been granted by the Ethics and Integrity Sub-Committee (EISC).

If you have any concerns regarding the conduct of the research in which you are being asked to participate, please contact:

Catherine Hitchens, Ethics, Integrity and Compliance Manager, Office for Postgraduates, Research and Engagement, University of East London, Docklands Campus, London, E16 2RD. Telephone: 020 8223 6683. Email: researchethics@uel.ac.uk

For general enquiries about the research please contact the Principal Investigator on the contact details at the top of this sheet.

Appendix B.3: Consent Form

Consent Form

UNIVERSITY OF EAST LONDON

Consent to Participate in a Programme Involving the Use of Human Participants.

Project Title: The Power of Dark Data - Exploring the Role of Data Governance

Please tick as appropriate:

	YES	NO
I have read the information leaflet relating to the above research project in which I have been asked to participate and have been given a copy to keep. The nature and purposes of the research project have been explained to me, and I have had the opportunity to discuss the details and ask questions about this information. I understand what is being proposed and the procedures in which I will be involved have been explained to me.		
I understand that my involvement in the research project, and particular data from this research, will remain strictly confidential as far as possible. Only the researchers involved in the research project will have access to the data.		
Where possible, participants' confidentiality will be maintained unless a disclosure is made that indicates that the participant or someone else is at serious risk of harm. Such disclosures may be reported to the relevant authority.		
Participants will be anonymised in publications that arise from the research.		
I give my permission for anonymised quotes from my responses to be used in publications resulting from the project.		
The results will be disseminated. Dissertation / Thesis, Peer reviewed journal, Written feedback to research participants, Books or chapters I give my permission for anonymised quotes from my responses to be used in the study and dissemination of research findings and / or publications resulting from the project.		

I understand that the data collected for the research project will be anonymised/pseudonymized before it is published.		
I understand that the published results of the research project will be accessible in the public domain and may be deposited in an open access data repository.		
I understand that the published results of the research project will be accessible in the public domain and may be re-used, republished, or reanalysed by others in future research.		
I give my permission for the research team to use the data that I have provided in future research projects which may be made publicly available.		
I agree to be contacted after submitting the required feedback for follow up questions and/or clarifications.		
It has been explained to me what will happen once the research project has been completed.		
I would like to receive the results of the final study for my personal use.		
I understand that my participation in this study is entirely voluntary, and I am free to withdraw at any time during the research without disadvantage to myself and without being obliged to give any reason. I understand that my data can be withdrawn up to the point of data analysis, and that after this point it may not be possible if the data is anonymised.		
I hereby freely and fully consent to participating in the study which has been fully explained to me and for the information obtained to be used in relevant research publications.		

Participant's Name (BLOCK CAPITALS)

.....

Participant's Signature

.....

Investigator's Name (BLOCK CAPITALS)

.....

Investigator's Signature

.....

Date:

Appendix C: Analysis of Key Challenges for Data Governance Implementation

The key challenges for data governance are presented below. The identified challenges provide a comprehensive and clear overview of the critical areas organisations must focus on to achieve effective data governance implementation. Each theme encompasses related challenges, allowing for a more strategic approach to addressing the complexities involved in managing data across modern enterprises. This thematic approach also highlights the interconnected nature of these challenges, emphasizing the need for holistic, adaptable, and continuously improving governance frameworks.

1. Standardization and Consistency

- **Lack of Standardization:** The absence of universally accepted standards complicates data governance implementation across organisations, leading to inconsistencies in data management practices (Abraham, Schneider, and Brocke, 2019).
- **Inconsistent Data Definitions:** Different departments within an organisation often have inconsistent data definitions, leading to miscommunication and complications in data governance (Wende, 2007).
- **Lack of Standardization Across Industries:** Varying standards for data governance across industries create challenges for organisations operating in multiple sectors, leading to inconsistencies in governance practices (Cheong and Chang, 2007).

2. Data Quality Management

- **Insufficient Data Quality:** Poor data quality remains a persistent issue, compromising the effectiveness of data governance efforts (Côte-Real, Ruivo, and Oliveira, 2020).
- **Ensuring Data Quality Across the Organisation:** Maintaining high data quality across various departments and systems is a continuous challenge, with inconsistent practices undermining data governance (Wang and Strong, 1996).
- **Addressing Data Quality Issues Across the Data Lifecycle:** Ensuring data quality throughout the entire data lifecycle is a persistent challenge that can undermine the effectiveness of governance initiatives (Lee et al., 2002).

3. Organisational Culture and Resistance

- **Organisational Resistance:** Resistance within the organisation, where employees perceive data governance as a burden or threat, can derail governance initiatives (Otto, 2011).
- **Cultural Barriers:** Organisational culture, including resistance to change and lack of data literacy, can undermine efforts to establish effective data governance (Cheong and Chang, 2007).
- **Cultural Resistance to Data Sharing:** Cultural resistance to sharing data across departments or with external partners hinders successful data governance (Weber, Otto, and Osterle, 2009).

4. Legal, Ethical, and Regulatory Compliance

- **Legal and Ethical Concerns:** Navigating complex legal and ethical landscapes, especially with growing data privacy regulations, is a formidable challenge for data governance (Thiel, Stroetmann, and Singleton, 2014).
- **Evolving Regulatory Requirements:** The continuously evolving regulatory environment around data introduces significant challenges in ensuring compliance (Al-Ruithe and Benkhelifa, 2017).

- Compliance with International Regulations: Global organisations face challenges in complying with various international data protection regulations, requiring adaptable governance frameworks (Thiel, Stroetmann, and Singleton, 2014).
- Ensuring Consistent Data Privacy: Stricter data privacy regulations require that data governance frameworks consistently uphold privacy standards across the organisation, which is particularly challenging for global organisations (Guetat and Dakhli, 2015).
- Ensuring Compliance with Data Localization Laws: Data localization laws, requiring data to be stored and processed within specific geographical boundaries, add complexity to global data governance frameworks (Gallaher et al., 2015).

5. Accountability and Ownership

- Fragmented Accountability: Unclear or fragmented accountability structures lead to inefficiencies and gaps in governance practices (Kooper, Maes, and Lindgreen, 2011).
- Data Ownership Confusion: Unclear ownership of data within an organisation leads to conflicts and poor data management practices (Niemi and Laine, 2016).
- Complexity of Data Ownership: Clarifying and managing data ownership in large organisations with complex data environments is challenging, often leading to disputes and governance issues (Khatri and Brown, 2010).
- Data Ownership in Complex Ecosystems: Defining and managing data ownership in complex ecosystems involving multiple stakeholders is complicated, requiring clear governance agreements (Gimpel, 2020).
- Addressing the Challenges of Data Ownership in Collaborative Environments: Collaborative environments, such as joint ventures or partnerships, complicate the definition and management of data ownership, requiring clear governance structures (Lavalle and Smilde, 2021).

6. Resource Allocation and Constraints

- Resource Constraints: Limited resources, including budget and skilled personnel, hinder the effective implementation of data governance programs, especially in smaller organisations (Weber, Otto, and Osterle, 2009).
- Lack of Skilled Personnel: A shortage of skilled personnel in data governance is a significant barrier, particularly in rapidly evolving technological landscapes (Lavalle and Smilde, 2021).
- Difficulty in Measuring ROI: Quantifying the return on investment (ROI) for data governance initiatives is challenging, making it difficult to secure ongoing investment (Redman, 2018).

7. Technological Changes and Integration

- Rapid Technological Changes: The fast pace of technological advancements, such as cloud computing and big data, requires continuous adaptation of data governance frameworks (Al-Ruithe, Benkhelifa, and Hameed, 2016).
- Legacy Systems Integration: Many organisations rely on legacy systems that do not support modern data governance practices, making integration into contemporary frameworks challenging (Olaitan, Herselman, and Wayi, 2016).
- Dealing with Legacy Systems: Legacy systems, which often do not comply with modern data governance standards, present significant challenges in integrating them into a unified governance framework (Ning, 2016).
- Evolution of Data Governance Practices: As organisations mature in their data governance efforts, evolving practices to keep up with new technologies and business needs requires continuous learning and adaptation (DAMA, 2017).

8. Complexity of Data Environments

- Complexity of Data Environments: The integration of legacy systems with modern platforms and the overall complexity of data environments add layers of difficulty to data governance (Benfeldt, 2017).
- Dynamic and Complex Data Landscapes: Managing diverse data types and sources, especially in real-time, adds to the complexity of data governance (Côte-Real, Ruivo, and Oliveira, 2020).
- Complexity in Data Integration: Integrating data from multiple sources, particularly in organisations with diverse systems, is complex and error-prone, complicating data governance (Gregory, 2011).
- Integration of Structured and Unstructured Data: Integrating both structured and unstructured data into a cohesive governance framework is challenging, requiring specialized approaches (Thomas, 2020).

9. Data Security and Risk Management

- Balancing Data Access and Security: Ensuring data accessibility while protecting it from unauthorized access is a critical challenge, requiring a balance between democratization and security (AlGhamdi, Win, and Vlahu-Gjorgievska, 2020).
- Ensuring Data Security: Safeguarding data from internal and external threats while ensuring accessibility is a continuous challenge that requires robust security measures (Alreemy et al., 2016).
- Transparency in Data Processing: Achieving transparency in data processing while maintaining efficient operations is increasingly important, particularly in the context of privacy regulations (Al-Ruithe, Benkhelifa, and Hameed, 2016).

10. Cross-Departmental Coordination and Collaboration

- Cross-Departmental Coordination: Effective data governance requires coordination across multiple departments, each with its own priorities and practices, making seamless collaboration difficult (Otto, 2011).
- Complexity in Cross-Functional Collaboration: Collaboration across functions like IT, legal, compliance, and business units is essential for data governance but is often challenging due to differing priorities and understandings (Weber, Otto, and Osterle, 2009).

11. Governance in Dynamic and Agile Environments

- Governance in Dynamic Environments: Rapidly changing business environments require adaptable data governance frameworks that can keep pace with technological advancements and shifting needs (Marus, 2018).
- Data Governance in Agile Environments: Implementing data governance in agile environments is challenging due to the need for flexibility in governance frameworks, which can conflict with structured governance requirements (Baškarada, Gao, and Koronios, 2006).

12. Mergers, Acquisitions, and Multi-Cloud Strategies

- Data Governance in Mergers and Acquisitions: Mergers and acquisitions introduce unique challenges for data governance as organisations must integrate disparate systems and frameworks, requiring complex and time-consuming alignment (Koooper, Maes, and Lindgreen, 2011).
- Data Governance in Multi-Cloud Environments: The adoption of multi-cloud strategies complicates data governance due to the need to manage data across different platforms with varying policies and controls (Al-Ruithe, Benkhelifa, and Hameed, 2018).

13. Data Lifecycle Management

- Data Lifecycle Management: Managing the entire lifecycle of data—from creation to deletion—is a challenge, as many organisations struggle with issues like data bloat and the retention of unnecessary data (Niemi, 2011).

14. Integration with Business Objectives

- Integration with Business Processes: Data governance must be well-integrated with core business processes to ensure that governance practices align with and support strategic decision-making and operations (Kooper, Maes, and Lindgreen, 2011).
- Ensuring Alignment with Business Objectives: Governance frameworks must align with overall business objectives to avoid practices that hinder strategic goals, ensuring the value of data governance initiatives (Otto, 2011).
- Misalignment with Business Strategy: Misaligned data governance initiatives that do not support business objectives can reduce the overall value derived from governance efforts (Curtiss, Saxena, and Seth, 2018).

15. Data Governance in Specialized Data Environments

- Data Governance in Big Data Environments: Managing governance in big data environments, characterized by high volume, velocity, and variety of data, requires new approaches that traditional models may not support (Jagals and Karger, 2021).
- Governance of External Data: Governing external data sources, such as those from third-party providers or partners, presents challenges in ensuring data quality and integration with internal systems (Wang and Strong, 1996).
- Managing the Governance of IoT Data: The rapid proliferation of IoT devices, which generate high volumes of often unstructured data, introduces new challenges in integrating this data into existing governance frameworks (Côte-Real, Ruivo, and Oliveira, 2020).
- Governance in the Context of AI and Machine Learning: Data governance must support AI and machine learning technologies while managing risks such as bias and data quality issues, which presents a complex challenge (Jagadish, 2022).

16. Real-Time Data Governance

- Real-Time Data Governance: The rise of real-time data processing and analytics demands governance frameworks that can operate at the same speed, often outpacing traditional models and leading to potential gaps (Bruck, 2017).
- Implementing Governance in Real-Time Data Environments: Traditional governance models often struggle to keep pace with the demands of real-time data environments, requiring adaptation for real-time analytics (Bruin and Solms, 2015).

17. Continuous Improvement and Adaptation

- Balancing Innovation and Control: Balancing the need for innovation with the need for control is crucial, as overly rigid governance can stifle creativity, while too much flexibility can lead to risks (Weber, Otto, and Osterle, 2009).
- Continuous Evolution of Data Governance Practices: As organisations evolve, so must their data governance practice, requiring ongoing adaptation and improvement to meet new technological and business demands (DAMA, 2017).
- Ensuring Stakeholder Buy-in: Gaining and maintaining support from stakeholders, including top management and data users, is crucial but challenging, as without buy-in, governance initiatives may lack the necessary resources and commitment (Hubbard, Freda, and Swanagan, 2020).
- Difficulty in Defining Data Policies: Crafting clear and enforceable data governance policies that balance accessibility, security, and compliance is complex and often leads to conflicting requirements (Loshin, 2010).

- Measuring Data Governance Effectiveness: Quantifying the effectiveness of data governance initiatives is difficult, as organisations struggle to establish metrics that accurately reflect the value provided by governance practices (Smallwood, 2012).
- Transparency and Adaptability in Governance: Governance frameworks must be transparent and adaptable to address evolving business needs and regulatory requirements while ensuring efficient operations (Al-Ruithe, Benkhelifa, and Hameed, 2016).

Appendix D: Analysis of Key Challenges for Dark Data Governance Implementation

The identified key challenges offer a comprehensive and clear examination of the critical areas that organisations must prioritize to successfully implement effective dark data governance. This structured approach facilitates a deeper understanding of the complex landscape of dark data governance. Each thematic category encompasses related challenges, enabling a strategic focus on the areas demanding the most attention in dark data governance. This thematic structure also underscores the necessity for continuous improvement, adaptability, and strong alignment with organisational goals and processes to effectively manage and leverage dark data within the enterprise.

1. Identification, Classification, and Retrieval of Dark Data

- **Identification and Classification:** Identifying and classifying dark data is a major challenge due to its hidden nature, making it difficult for organisations to leverage these assets effectively (Deloitte, 2017).
- **Identification and Retrieval of Dark Data:** Retrieving dark data from across the organisation is challenging due to its often hidden or forgotten state in various systems (Heidorn, 2008).
- **Lack of Visibility:** The hidden nature of dark data within an organisation's ecosystem complicates the implementation of effective governance strategies (McNulty, 2017).

2. Data Security, Privacy, and Ethical Concerns

- **Data Security Risks:** Unmanaged dark data poses significant security risks, potentially leading to breaches and compliance issues (Al-Ruithe, Benkhelifa, and Hameed, 2018).
- **Data Sensitivity and Privacy Risks:** Dark data may contain sensitive information that was not originally flagged, raising challenges in ensuring compliance with privacy regulations (Thiel, Stroetmann, and Singleton, 2014).
- **Ethical and Privacy Concerns:** Managing dark data ethically, particularly when it contains sensitive or personal information, presents significant governance challenges (Lavalle and Smilde, 2021).
- **Ethical Concerns Around the Use of Dark Data:** The potential use of dark data containing sensitive information raises ethical concerns that organisations must navigate carefully (Cheng, 2018).
- **Ethical Challenges in Data Repurposing:** Repurposing dark data collected for one purpose for another can raise ethical concerns, especially without the consent of data subjects (Meghji, 2017).
- **Legal and Regulatory Uncertainty:** Dark data often includes information collected without clear consent or under outdated regulations, complicating governance and compliance (Lavalle and Smilde, 2021).
- **Uncertain Legal Implications:** The unclear legal status of dark data, especially if collected under outdated regulations, presents challenges in governance and compliance (Gimpel, 2020).
- **Privacy Concerns with Hidden Data:** Dark data can inadvertently contain personally identifiable information (PII), complicating efforts to ensure privacy and compliance with regulations (Johnson, 2020).

3. High Costs and Resource Constraints

- **High Costs of Management:** Managing dark data is resource-intensive, requiring significant investment in storage, processing, and analysis (Cheng, Su, and Shen, 2023).

- **High Costs of Processing and Analysing Dark Data:** The expense of processing and analysing dark data often outweighs the uncertain benefits, making it challenging for organisations to justify these costs (Snowflake, 2019).
- **Storage Costs for Unused Data:** Storing dark data, especially when its value is uncertain, can be prohibitively expensive, leading organisations to weigh the costs against potential benefits (Splunk, 2019).
- **Uncertainty in Long-Term Data Storage:** Storing dark data over the long term presents challenges related to cost, security, and data degradation, requiring careful assessment of trade-offs (Cafarella et al., 2016).
- **Hidden Costs:** Organisations often underestimate the hidden costs associated with dark data, such as storage, security, and compliance risks (Gartner, 2020).
- **Resource Constraints in Managing Dark Data:** Managing and governing dark data requires significant resources, including time, money, and expertise, which many organisations struggle to allocate (Budgen et al., 2018).

4. Integration and Interoperability Challenges

- **Integration with Existing Data Governance Frameworks:** Integrating dark data governance into existing frameworks is complex due to the distinct characteristics of dark data (McNulty, 2017).
- **Integrating Dark Data with Mainstream Data:** The differences in format, structure, and quality between dark and structured data complicate the integration necessary for comprehensive analysis (Cafarella et al., 2016).
- **Data Interoperability Issues:** Dark data often exists in outdated or incompatible formats, making it difficult to integrate with modern data systems (Cheng et al., 2017).

5. Tools, Technology, and Automation

- **Inadequate Tools for Analysis:** Traditional data analysis tools are often insufficient for managing large volumes of unstructured dark data, limiting organisations' ability to fully leverage these assets (Cafarella et al., 2016).
- **Lack of Tools for Analysing Dark Data:** Many organisations lack the necessary tools and technologies to analyse dark data effectively, leaving valuable data underutilized (Cafarella et al., 2016).
- **Challenges in Automating Dark Data Governance:** The unstructured nature of dark data makes it difficult to automate governance processes, leading to reliance on manual, time-consuming methods (Hinkle, 2020).

6. Data Quality, Redundancy, and Cleansing

- **Data Redundancy and Duplication:** Dark data often includes redundant or duplicate information, complicating governance and increasing storage costs (Karande et al., 2019).
- **Data Duplication and Redundancy:** Identifying and managing duplicated dark data is necessary to streamline governance efforts and reduce unnecessary storage (Trajanov et al., 2018).
- **Challenges in Data Cleansing:** Cleansing dark data of inaccuracies, duplicates, and irrelevant information is a time-consuming and resource-intensive process (Heidorn, 2008).
- **Data Decay and Data Integrity:** Over time, dark data can become outdated or lose its integrity, complicating governance and reducing its utility (Gallaher et al., 2015).

7. Legal and Ethical Compliance Risks

- **Legal Risks of Unanalysed Data:** Dark data may contain information that could lead to legal liabilities if uncovered during audits or inspections, presenting compliance challenges (Thiel, Stroetmann, and Singleton, 2014).

- Unforeseen Legal Risks: Dark data can expose organisations to unforeseen legal risks due to the lack of active governance and regular review (Rees, 2020).
- Legal and Ethical Dilemmas in Data Retention: Retaining dark data for long periods raises ethical concerns, particularly regarding the storage of personal or sensitive information and may expose organisations to unforeseen legal risks (Cafarella et al., 2016).

8. Adaptability, Agility, and Change Management

- Evolving Nature of Dark Data: The continuous generation of new data requires ongoing efforts to identify, classify, and govern dark data, making governance a moving target (Sundarraaj and Natrajan, 2019).
- Adaptability and Change Management: Governing dark data effectively requires organisations to adapt to the evolving nature of data and implement changes to governance practices as necessary (Cheng, 2018).
- Difficulty in Predicting Data Value: The unknown nature of dark data makes it challenging to predict its value, requiring organisations to be agile in their approach to governance (Lavallo and Smilde, 2021).

9. Data Categorization and Metadata Management

- Complexity in Data Categorization: Dark data, often in unstructured formats, is difficult to categorize, complicating governance and compliance efforts (Trajanov et al., 2018).
- Incomplete or Missing Metadata: Dark data frequently lacks necessary metadata, making it difficult to understand its context and relevance for governance (Veaux and Hand, 2005).

10. Coordination and Common Knowledge

- Fragmented Data Sources: Dark data often originates from multiple fragmented sources, making it difficult to compile and govern effectively (Heidorn, 2008).
- Lack of Accountability: The absence of clear accountability for dark data governance leads to unmanaged data, increasing risks (Alreemy et al., 2016).
- Lack of Awareness: Many organisations are unaware of the extent and potential value of their dark data, leading to underinvestment in governance strategies (Jagadish, 2022).
- Limited Awareness of Dark Data Risks: The risks associated with dark data, including security vulnerabilities and compliance issues, are often underestimated by organisations (McNulty, 2017).
- Lack of Organisational Commitment: Effective dark data governance requires strong commitment from leadership, which is often lacking, leading to underfunded and deprioritized efforts (Cheng, Su, and Shen, 2023).

11. Supporting Business Processes and Goals

- Uncertainty of Data Value: The uncertainty surrounding the value of dark data makes it difficult for organisations to justify the data governance costs and efforts required to support the business processes and organisational goals (McNulty, 2017).
- Uncertainty in Data Governance Outcomes: The hidden nature of dark data leads to uncertain outcomes in governance efforts, making it difficult to justify investments in data governance to support the business processes and organisational goals (Lavallo and Smilde, 2021).
- Difficulty in Prioritizing Data: Organisations struggle to prioritize dark data for analysis and governance, leading to resource allocation challenges to data governance requirements. This impacts the data governance support to business processes and organisational goals (Lavallo and Smilde, 2021).
- Data Access and Security Controls: Implementing effective access and security controls for dark data is challenging because it often resides in less visible areas of an organisation's IT infrastructure. This creates a challenge for data governance function

at large in supporting the business processes and organisational goals (Smallwood, 2012).

- Risk of Data Mismanagement: Without proper governance, dark data can be easily mismanaged, leading to breaches or loss of valuable information. This creates a challenge for data governance function at large in supporting the business processes and organisational goals (Gallaher et al., 2015).
- Emerging Threats and Risks: As cyber threats evolve, ensuring that dark data is adequately protected becomes increasingly challenging. This creates a challenge for data governance function at large in supporting the business processes and organisational goals (McNulty, 2017).

12. Corporate Policies and Data Architecture

- Governance of Data in Non-Traditional Formats: Dark data often exists in non-traditional formats like logs, images, and audio files, which are harder to govern using traditional tools. This is a challenge to build common organisational data architecture and develop corporate policies (Gartner, 2020).
- Governance of Dark Data in Legacy Systems: Legacy systems often lack modern data management features, making it difficult to govern dark data effectively under common architecture and unified corporate policies (Otto, 2011).

13. Data Integration and Interoperability

- Data Interoperability Issues: Ensuring that dark data, often in outdated formats, can be accessed and used alongside current data sets is a significant governance challenge (Cheng et al., 2017).
- Difficulty in Data Deletion: Organisations often hesitate to delete dark data due to fears of losing valuable information or facing compliance issues, complicating data integration (Snowflake, 2019).

14. Extracting Value from Data

- Risk of Data Misinterpretation: The unstructured and unorganised nature of dark data increases the risk of misinterpretation, leading to poor decision-making (Hummel, 2014).
- Data Relevance and Usefulness: Determining the relevance and usefulness of dark data is challenging, as not all dark data is valuable, making it difficult to sift through large volumes to find actionable insights (Judah and White, 2021).
- Extracting Insights from Unstructured Data: Dark data often consists of unstructured formats like text, video, and audio, requiring advanced tools to extract valuable insights (Karande et al., 2019).

15. Continuous Improvement and Learning

- Ongoing Learning and Adaptation: Governing dark data effectively requires continuous learning and adaptation to keep pace with evolving data types, technologies, and business needs (Cheng, 2018).
- Ongoing Efforts to Identify and Govern: The dynamic nature of dark data necessitates ongoing efforts to identify, classify, and govern this data, making it a continuous challenge (Sundarraaj and Natrajan, 2019).

Appendix E: Analysis of Critical Success Factors (CSFs) for Data Governance Implementation

The following structured critical success factors for data governance are focused on supporting key business operations and enabling the achievement of organisational goals. These CSFs provide a foundational basis for the successful implementation of comprehensive data governance programs within organisations.

1. Clear Data Governance Purpose to Support Business Processes and Objectives

- **Defined Data Governance Framework:** Establishing a comprehensive framework is fundamental to guide all data governance activities, ensuring consistency and alignment with business objectives (Abraham, Schneider, and Brocke, 2019).
- **Integration with Business Strategy:** Data governance must be closely aligned with the organisation's overall business strategy to ensure that data management practices support and enhance business objectives (Weber, Otto, and Osterle, 2009).
- **Strategic Data Governance Vision:** Establishing a clear vision for data governance helps in guiding the organisation's data governance efforts and ensuring alignment with long-term business goals (Weber, Otto, and Osterle, 2009).

2. Clarity on Business Scope and Data Scope

- **Data Stewardship:** Appointing data stewards ensures that data is managed effectively throughout its lifecycle, from creation to disposal, while maintaining its integrity within a defined business scope (DAMA, 2017).
- **Data Lifecycle Management:** Managing the data lifecycle as per business requirements from creation to retirement ensures that data remains relevant to business and compliant with regulatory requirements throughout its existence (HNU, 2020).
- **Data Classification Standards:** Establishing data classification standards helps in organizing data based on its sensitivity and value to business processes, ensuring that it is managed and protected appropriately (Weber, Otto, and Osterle, 2009).
- **Comprehensive Data Inventory:** Maintaining a comprehensive inventory of data assets helps in organizing, managing, and protecting data, which is essential for effective data governance that supports business operations (Collibra, 2020).

3. Business Compliance with Data Governance

- **Regulatory Compliance:** Adhering to regulatory requirements not only ensures legal compliance but also protects the organisation from potential legal and financial penalties (Al-Ghamdi, Win, and Vlahu-Gjorgievska, 2020).
- **Privacy Management:** Implementing privacy management practices ensures that data governance activities comply with privacy laws and regulations, protecting individuals' data rights (Gallaher et al., 2015).
- **Legal Compliance for Data Management:** Ensuring that data management practices comply with all relevant laws and regulations helps in protecting the organisation from legal risks and ensuring the integrity of its data governance initiatives (Thiel, Stroetmann, and Singleton, 2014).
- **Data Governance in Regulatory Environments:** Implementing data governance practices that comply with regulatory requirements helps in protecting the organisation from legal risks and penalties (Al-Ghamdi, Win, and Vlahu-Gjorgievska, 2020).

4. Coordination and Harmonization

- **Stakeholder Engagement:** Active involvement of stakeholders across all levels promotes buy-in and ensures that data governance initiatives are aligned with the needs and expectations of the business (Alreemy et al., 2016).

- **Cross-functional Collaboration:** Encouraging collaboration across different functions and departments enhances the effectiveness of data governance by ensuring that all perspectives and needs are considered (Alreemy et al., 2016).
- **Data Governance Committee:** Establishing a data governance committee function helps in overseeing data governance activities, ensuring alignment with business goals, and resolving any governance-related issues (Niemi, 2011).
- **Effective Communication:** Regular and transparent communication about data governance policies, roles, and expectations is vital for ensuring that all stakeholders are informed and engaged (Alreemy et al., 2016).
- **Data Governance Communication Strategy:** Developing a clear communication strategy helps in ensuring that all stakeholders are informed about data governance policies, practices, and expectations, which enhances transparency and compliance (Alreemy et al., 2016).
- **Effective Data Communication:** Ensuring that communication strategies for data governance are clear and actionable helps in managing risks associated with unstructured or hidden data (Alreemy et al., 2016).
- **Engagement with Regulatory Bodies:** Actively engaging with regulatory bodies helps in staying informed about changes in regulations and ensuring that data governance practices remain compliant with current legal requirements (Thiel, Stroetmann, and Singleton, 2014).
- **Legal Compliance Communication:** Establishing clear channels for communicating legal compliance requirements across the organisation helps in ensuring that all stakeholders understand and adhere to relevant regulations (Thiel, Stroetmann, and Singleton, 2014).

5. Corporate Control and Cohesion

- **Data Access Control:** Implementing robust common data access controls protects sensitive data from unauthorized access, ensuring data security and compliance with privacy regulations across the organisation to ensure cohesion (Gallaher et al., 2015).
- **Corporate Data Ownership and Custodianship:** Clearly defining ownership and custodianship corporate roles ensures that there is accountability for data across its lifecycle, enhancing data governance practices across the organisation (Weber, Otto, and Osterle, 2009).
- **Incident Management and Response:** Establishing incident management procedures helps in quickly addressing and controlling data governance breaches or issues, minimizing their impact on the organisation (Bruck, 2017).
- **Resource Allocation for Data Governance:** Allocating sufficient resources to data governance initiatives at corporate level ensures that they are effectively implemented and sustained over time (Niemi, 2011).
- **Data Governance Process Documentation:** Documenting data governance processes helps in ensuring consistency, providing a reference for stakeholders, and supporting compliance with regulatory requirements at the corporate level. This ensures cohesion (Niemi, 2011).
- **Support from Executive Leadership:** Securing support from executive leadership is crucial for the success of corporate data governance initiatives. This helps in securing resources, driving adoption, and aligning governance with business goals to ensure cohesion (Weber, Otto, and Osterle, 2009).

6. Corporate Policies for Key Data Governance Domains

- **Data Quality Management:** Implementing rigorous data quality standards ensures the accuracy, completeness, and reliability of data, which are critical for effective decision-making (Côte-Real, Ruivo, and Oliveira, 2020).

- **Metadata Management:** Effective metadata management helps in understanding the context, content, and structure of data, which is critical for data quality, retrieval, and governance (Otto, 2011).
- **Master Data Management (MDM):** Implementing MDM practices helps in maintaining consistent and accurate master data across the organisation, which is critical for effective data governance (Stedman and Vaughan, 2020).
- **Data Retention and Archiving Policies:** Developing clear policies for data retention and archiving ensures that data is stored appropriately and is accessible when needed, while also complying with regulatory requirements (Weber, Otto, and Osterle, 2009).
- **Policy Development and Enforcement:** Developing and enforcing clear data governance policies ensures consistent application of data management practices across the organisation (Niemi, 2011).
- **Data Usage Policies:** Developing and enforcing clear data usage policies ensures that data is used appropriately and ethically, supporting the organisation's data governance objectives (Weber, Otto, and Osterle, 2009).
- **Ethical Data Use:** Promoting ethical data use ensures that data is managed and utilized in ways that are consistent with legal, ethical, and organisational standards (Thiel, Stroetmann, and Singleton, 2014).
- **Data Policy Management:** Effectively managing data policies ensures that they are up-to-date, aligned with business goals, and enforced consistently across the organisation, which is critical for successful data governance (Loshin, 2010).

7. Audit and Compliance Monitoring

- **Continuous Monitoring and Auditing:** Regular monitoring and auditing of data governance processes ensure that they remain effective and compliant with internal and external standards (Brous, Janssen, and Vilminko-Heikkinen, 2016).
- **Data Protection Impact Assessments:** Conducting regular data protection impact assessments helps in identifying potential risks to data privacy and security, ensuring compliance with regulatory requirements (Thiel, Stroetmann, and Singleton, 2014).
- **Auditable Data Governance Processes:** Ensuring that data governance processes are auditable helps in demonstrating compliance with internal and external standards, which is essential for maintaining trust and accountability (Brous, Janssen, and Vilminko-Heikkinen, 2016).
- **Vendor and Third-Party Data Governance:** Ensuring that vendors and third parties comply with the organisation's data governance policies helps in protecting data across the entire supply chain and reducing risks associated with external partnerships (Al-Ruithe, Benkhelifa, and Hameed, 2018).

8. Adaptation and Intelligence

- **Agility in Data Governance:** Implementing agile data governance practices allows organisations to quickly adapt to changes in the data landscape, ensuring that governance practices remain relevant and effective (Baškarada, Gao, and Koronios, 2006).
- **Adaptation to Environmental Changes:** Organisations must be agile and responsive to changes in the external environment, including new regulations, emerging technologies, and shifting market dynamics, to sustain their data governance initiatives (Brous, Janssen, and Vilminko-Heikkinen, 2016).
- **Adoption of Industry Best Practices:** Adopting best practices from industry leaders helps in ensuring that data governance practices are effective, efficient, and aligned with global standards (DAMA, 2017).

- **Proactive Data Governance:** Taking a proactive approach to managing risks associated with data governance helps in preventing potential issues and ensuring the resilience of governance practices (Al-Ghamdi, Win, and Vlahu-Gjorgievska, 2020).
- **Agile Governance:** Implementing governance structures that are agile and responsive to changes in the data environment, ensuring adaptability and resilience (Weber, Otto, and Osterle, 2009).
- **Effective Data Governance Leadership:** Strong leadership in data governance helps in driving governance initiatives, securing resources, and ensuring alignment with short- and long-term organisational goals to support adaptation (DAMA, 2017).

9. Integrated Governance

- **Integration with IT Governance:** Aligning data governance with IT governance ensures that data management practices are integrated with the organisation's IT infrastructure and processes, leading to more efficient and effective governance (Alreemy et al., 2016).
- **Data Integration and Interoperability:** Ensuring that data governance practices facilitate the integration and interoperability of data across different systems and platforms enhances data usability and governance (Otto, 2011).
- **Integration of Data Governance in Cloud Environments:** Adapting data governance practices for cloud environments ensures that data remains secure and compliant when stored or processed in the cloud (Al-Ruithe, Benkhelifa, and Hameed, 2018).
- **Integration with Enterprise Architecture:** Aligning data governance with enterprise architecture ensures that data management practices are integrated into the broader IT and business infrastructure, enhancing overall governance (Guetat and Dakhli, 2015).
- **Data Governance for Data Analytics:** Implementing data governance practices tailored to data analytics high-tech initiatives ensures that data used for analytics is accurate, consistent, and secure, supporting better decision-making (Côte-Real, Ruivo, and Oliveira, 2020).
- **Effective Governance of Big Data Initiatives:** Implementing data governance practices tailored to big data high-tech initiatives ensures that large and complex datasets are managed effectively and securely (Côte-Real, Ruivo, and Oliveira, 2020).

10. Learning, and Change Management

- **Change Management:** Successfully managing changes in data governance practices involves preparing, supporting, and helping individuals, teams, and the organisation to adapt to changes (Mento, 2002).
- **Effective Data Stakeholders Training:** Providing training for data stakeholders ensures that they have the skills and knowledge needed to manage data effectively, which is essential for effectively implementing data governance functions (DAMA, 2017).

11. Governance Common Knowledge

- **Metadata Management:** Effective metadata management helps in understanding the context, content, and structure of data, which is critical for data quality, retrieval, and governance (Otto, 2011).
- **Standardized Data Definitions:** Establishing standardized definitions for key data elements ensures that all stakeholders have a common understanding of data, which is essential for data quality and consistency (Weber, Otto, and Osterle, 2009).

12. Continuous Improvements for Data Governance

- **Continuous Monitoring and Auditing:** Regular monitoring and auditing of data governance processes ensure that they remain effective and compliant with internal and external standards (Brous, Janssen, and Vilminko-Heikkinen, 2016).
- **Data Governance Metrics and KPIs:** Defining and tracking key performance indicators (KPIs) for data governance allows organisations to measure the effectiveness of their

governance initiatives and make informed improvements (Curtiss, Saxena, and Seth, 2018).

- **Monitoring Data Governance Effectiveness:** Regularly monitoring and assessing the effectiveness of data governance practices helps in identifying areas for improvement and ensuring that governance initiatives remain aligned with organisational goals (Curtiss, Saxena, and Seth, 2018).
- **Long-Term Data Governance Strategy:** Developing a long-term strategy for data governance helps in ensuring that governance practices are sustainable, adaptable, and aligned with the organisation's future goals (Weber, Otto, and Osterle, 2009).
- **Continuous Improvements for Data Governance:** Establishing a process for ongoing evaluation and improvement of data governance practices ensures that they remain relevant and effective (Brous, Janssen, and Vilminko-Heikkinen, 2016).
- **Data Governance Maturity Model Assessment:** Regularly assessing the maturity of data governance practices helps organisations understand their current state and identify areas for improvement (HNU, 2020).
- **Continuous Improvement Process:** Establishing a process for continuous improvement ensures that data governance practices are regularly evaluated and enhanced based on lessons learned and evolving needs (Brous, Janssen, and Vilminko-Heikkinen, 2016).

Appendix F: Analysis of Critical Success Factors (CSFs) for Dark Data Governance Implementation

The following structured critical success factors for dark data governance are focused on supporting key business operations and enabling the achievement of organisational goals. These CSFs provide a foundational framework for the successful implementation of comprehensive dark data governance programs within organisations.

1. Dark Data Governance Purpose to Support Business Processes and Goals

- Integration of Dark Data with Business Strategy: Aligning dark data governance with the organisation's business strategy ensures that dark data is leveraged to support business goals and drive value creation (Lavalle and Smilde, 2021).
- Strategic Utilization of Dark Data: Developing strategies to utilize dark data for business intelligence, innovation, and other strategic purposes helps in unlocking its value and driving competitive advantages (Agrawal, 2019).
- Ensuring Data Governance Alignment with Business Needs: Aligning dark data governance with the organisation's business needs helps in ensuring that governance efforts are focused on areas that will drive the most value and support strategic goals (Lavalle and Smilde, 2021).

2. Business Scope, Data Scope, and Dark Data Classifications

- Identification of Dark Data Sources: Identifying sources of dark data within the organisation is the first step in managing it effectively (Ajis and Baharin, 2019).
- Classification of Dark Data: Classifying dark data based on its sensitivity, value, and relevance to business helps in prioritizing data management efforts and ensuring that the most critical data is managed appropriately within the defined business scope. (Gartner, 2020).

3. Business operations Compliance with Dark Data Governance functions

- Compliance with Data Protection Laws: Ensuring that dark data management practices by business operations comply with relevant data protection laws and regulations helps in mitigating legal risks across the organisation (Thiel, Stroetmann, and Singleton, 2014).
- Dark Data Governance Compliance: Conducting regular compliance audits for dark data ensures that governance practices implemented by business operations are aligned with legal requirements (Brous, Janssen, and Vilminko-Heikkinen, 2016).
- Addressing Dark Data Privacy Concerns: Implementing measures to address privacy concerns related to dark data helps in protecting individuals' data rights and ensuring compliance with privacy regulations (Thiel, Stroetmann, and Singleton, 2014).
- Developing Dark Data Best Practices: Establishing and promoting best practices by business operations for dark data governance helps in ensuring that this data is managed effectively, securely, and in alignment with industry standards (Lavalle and Smilde, 2021).
- Dark Data Retention and Disposal Policies: Developing and enforcing clear policies for the retention and disposal of dark data helps in managing storage costs, reducing risks, and ensuring compliance with regulatory requirements (Weber, Otto, and Osterle, 2009).
- Legal Frameworks for Dark Data: Developing and implementing legal frameworks for dark data governance helps in ensuring compliance with data protection laws by business operations and reducing legal risks (Thiel, Stroetmann, and Singleton, 2014).

- Mitigating Dark Data Legal Risks: Developing strategies to mitigate legal risks associated with dark data, such as privacy violations or breaches of data protection laws, is crucial for protecting the organisation and ensure compliance (Thiel, Stroetmann, and Singleton, 2014).
- Ethical Considerations in Dark Data Management: Addressing ethical issues related to dark data, such as privacy concerns and data misuse, is crucial for maintaining trust and ensuring compliance with ethical standards (Thiel, Stroetmann, and Singleton, 2014).

4. Coordination and Harmonization

- Cross-Departmental Collaboration for Dark Data: Encouraging collaboration across departments ensures that dark data is managed consistently and effectively (Ajis and Baharin, 2019).
- Cross-functional Dark Data Governance Teams: Establishing cross-functional teams for dark data governance ensures that different perspectives and expertise are considered in the management of dark data (Ajis and Baharin, 2019).
- Integration with Existing Data Governance: Integrating dark data governance with the organisation's existing data governance framework ensures consistency and avoids duplication of efforts (Lavalle and Smilde, 2021).
- Effective Dark Data Communication: Developing a communication strategy for dark data governance ensures that all stakeholders are informed about policies, practices, and risks associated with dark data (Alreemy et al., 2016).
- Engagement with Regulatory Bodies: Actively engaging with regulatory bodies helps in staying informed about changes in regulations and ensuring that dark data governance practices remain compliant with current legal requirements (Thiel, Stroetmann, and Singleton, 2014).

5. Control, Cohesion, and Corporate Policies Development

- Developing Dark Data Governance Policies: Establishing clear policies for the governance of dark data ensures that it is managed consistently and effectively across the organisation (Gartner, 2020).
- Dark Data Governance Framework Development: Developing a comprehensive framework for the governance of dark data ensures that it is managed systematically and consistently across the organisation (Gartner, 2020).
- Establishing Dark Data Governance Roles: Defining specific roles and responsibilities for dark data governance ensures that this data is managed effectively and that there is accountability at every stage (DAMA, 2017).
- Automation of Dark Data Governance Processes: Implementing automation in dark data governance processes helps in reducing manual effort, increasing efficiency, and ensuring consistency (Lavalle and Smilde, 2021).
- Data stakeholders in Dark Data Governance: Appointing data stakeholders specifically for dark data helps in ensuring that this data is managed effectively and consistently, with clear accountability for its governance (DAMA, 2017).
- Establishing a Dark Data Governance Office: Setting up a dedicated office for dark data governance helps in centralizing governance efforts, ensuring consistency, and providing a focal point for managing dark data (DAMA, 2017).
- Dark Data Quality Control: Implementing policies and quality control measures for dark data ensures that it is accurate, consistent, and reliable, which is essential for its effective use in analytics and decision-making (Côte-Real, Ruivo, and Oliveira, 2020).
- Data Security in Dark Data Handling: Implementing robust data security policies and measures for dark data helps in protecting it from unauthorized access, breaches, and other security threats (Al-Ghamdi, Win, and Vlahu-Gjorgievska, 2020).

- **Retention Policies for Dark Data:** Developing and enforcing retention policies for dark data ensures that it is stored for appropriate periods and disposed of when no longer needed by the business operations (Weber, Otto, and Osterle, 2009).
- **Ensuring Data Accuracy and Relevance:** Implementing processes to ensure the accuracy and relevance of dark data helps in maximizing its value for business operations and ensuring that it supports informed decision-making (Côte-Real, Ruivo, and Oliveira, 2020).
- **Resource Allocation for Dark Data Management:** Allocating sufficient resources for dark data management ensures that the organisation can effectively control and manage this data, including storage, processing, and analysis (Sun, Su, and Shen, 2023).

6. Audit and Compliance Monitoring

- **Dark Data Audit Trails:** Establishing audit trails for dark data helps in tracking how this data is accessed, used, and managed, which is essential for ensuring compliance and accountability (Brous, Janssen, and Vilminko-Heikkinen, 2016).
- **Regular Dark Data Policy Reviews:** Conducting regular reviews of dark data governance policies helps in ensuring that they remain up-to-date, relevant, and effective in the face of changing regulations, technologies, and business needs (Weber, Otto, and Osterle, 2009).
- **Monitoring Dark Data Governance Effectiveness:** Regularly monitoring and assessing the effectiveness of dark data governance practices helps in identifying areas for improvement and ensuring that governance initiatives remain aligned with organisational goals (Curtiss, Saxena, and Seth, 2018).
- **Dark Data Governance Metrics and KPIs:** Defining and tracking metrics and KPIs for dark data governance helps in measuring the effectiveness of governance efforts and identifying areas for improvement (Curtiss, Saxena, and Seth, 2018).

7. Adaptation and Intelligence

- **Alignment with Organisational Strategic Goals:** Ensuring that dark data governance is aligned with the organisation's overall objectives helps in maximizing the value of this data and ensuring that it supports strategic goals (Lavalle and Smilde, 2021).
- **Adaptation to Environmental Changes:** Organisations must be agile and responsive to changes in the external environment, including new regulations, emerging technologies, and shifting market dynamics (Sun, Su, and Shen, 2023).
- **Leveraging Dark Data for Competitive Advantage:** Developing strategies to leverage dark data for competitive advantage helps in unlocking its value, identifying new opportunities, and differentiating the organisation in the market (Agrawal, 2019).
- **Long-Term Strategy for Dark Data:** Developing a long-term strategy for managing dark data helps in ensuring that governance practices are sustainable and adaptable to future changes in the data landscape (Weber, Otto, and Osterle, 2009).
- **Leveraging Dark Data for Competitive Advantage:** Developing strategies to leverage dark data for competitive advantage helps in unlocking its value, identifying new opportunities, and differentiating the organisation in the market (Agrawal, 2019).
- **Risk Assessment for Dark Data:** Conducting a thorough risk assessment for dark data helps in identifying potential threats and vulnerabilities and counteracting such risks (Sun, Su, and Shen, 2023).
- **Proactive Risk Management in Dark Data Initiatives:** Developing and implementing risk management strategies for dark data initiatives helps in identifying and mitigating potential risks (Sun, Su, and Shen, 2023).
- **Regular Dark Data Policy Reviews:** Conducting regular reviews of dark data governance policies helps in ensuring that they remain up-to-date, relevant, and

effective in the face of changing regulations, technologies, and business needs (Weber, Otto, and Osterle, 2009).

- Agility in Dark Data Governance: Implementing agile governance practices for dark data allows organisations to quickly adapt to changes in the data landscape (Lavalle and Smilde, 2021).

8. Integrated Governance

- Integration with Corporate Strategy: Aligning dark data governance with the organisation's corporate strategy ensures that governance efforts are focused on areas that will drive the most value and support long-term business objectives (Lavalle and Smilde, 2021).
- Integration with IT Infrastructure: Ensuring that dark data governance practices are integrated with the organisation's IT infrastructure helps in streamlining data management processes and ensuring consistency across the organisation (Weber, Otto, and Osterle, 2009).
- Dark Data Governance in Cloud Environments: Adapting dark data governance practices for cloud environments helps in ensuring that dark data stored or processed in the cloud is secure, compliant, and effectively managed (Al-Ruithe, Benkhelifa, and Hameed, 2018).
- Integration of Dark Data into Big Data Analytics: Ensuring that dark data is integrated into big data analytics high-tech initiatives helps in maximizing the value of all available data and supporting more comprehensive analytics and insights (Lavalle and Smilde, 2021).

9. Corporate Learning, and Change Management

- Change Management in Dark Data Governance: Successfully managing changes in dark data governance practices involves preparing, supporting, and helping individuals, teams, and the organisation to adapt to changes (Mento, 2002).
- Regular Training on Dark Data: Providing regular training on dark data governance helps in ensuring that employees are aware of the latest practices, technologies, and regulations related to dark data (DAMA, 2017).
- Creating Dark Data Awareness Programs: Developing and implementing awareness programs on dark data helps in educating employees about the importance of managing and protecting dark data (DAMA, 2017).
- Cross-functional Dark Data Governance Teams: Establishing cross-functional teams for dark data governance ensures that different perspectives and expertise are considered in the management of dark data (Ajis and Baharin, 2019).
- Transparent Dark Data Practices: Promoting transparency in dark data management practices helps in building trust with stakeholders and ensuring that the organisation's data governance activities are understood and supported (Lavalle and Smilde, 2021).
- Creating a Culture of Dark Data Awareness: Promoting a culture of awareness around dark data helps in ensuring that all employees understand the importance of managing and protecting this data (Weber, Otto, and Osterle, 2009).

10. Continuous Improvements for Dark Data Governance

- Continuous Monitoring of Dark Data: Regular monitoring of dark data helps in identifying new sources of dark data and ensuring that it is managed effectively over time (Wiebe and Allison, 2015).
- Dark Data Governance Metrics and KPIs: Defining and tracking metrics and KPIs for dark data governance helps in measuring the effectiveness of governance efforts and identifying areas for improvement (Curtiss, Saxena, and Seth, 2018).
- Continuous Improvement of Dark Data Practices: Establishing a process for continuous improvement in dark data governance helps in ensuring that governance practices are

regularly evaluated and enhanced based on lessons learned and evolving needs (Brous, Janssen, and Vilminko-Heikkinen, 2016).

- Understanding the Value of Dark Data: Conducting assessments to understand the potential value of dark data helps in prioritizing data management efforts and ensuring that valuable insights are not overlooked (Lavalle and Smilde, 2021).

Appendix G: Consolidated Critical Success Factors (CSFs) for Dark Data Governance Implementation

The comprehensive consolidation presented below covers all critical success factors across both data governance and dark data governance, ensuring that each key theme is thoroughly addressed and seamlessly integrated into a cohesive and highly effective governance strategy. By concentrating on these critical success factors, organisations can develop comprehensive and resilient governance frameworks that are closely aligned with their strategic goals, capable of adapting to evolving environmental and operational circumstances, and positioned to extract optimal value from all data assets while effectively managing dark data within the organisational context. Implementing a robust data governance program anchored in these key factors can enable enterprises to harness the full potential of their data resources, including dark data, in support of their overarching business objectives. This approach helps organisations establish a strong, sustainable data management foundation while counteracting dark data that is responsive to changing needs and empowers data-driven decision-making and innovation across the organisation.

1. Strategic Alignment and Purpose:

Data Governance and Dark Data Governance Purpose to Support Business Processes and Objectives:

- **Defined Data Governance Framework:** Establish comprehensive frameworks that guide all data governance activities, ensuring consistency and alignment with organisational objectives (Abraham, Schneider, and Brocke, 2019; Gartner, 2020).
- **Integration with Business Strategy:** Align data governance and dark data governance closely with the organisation's overall business strategy to ensure that data management practices support and enhance business objectives (Weber, Otto, and Osterle, 2009; Lavallo and Smilde, 2021).
- **Strategic Data Governance Vision:** Establishing a clear vision for data governance helps in guiding the organisation's data governance efforts and ensuring alignment with long-term business goals (Weber, Otto, and Osterle, 2009).
- **Ensuring Data Governance Alignment with Business Needs:** Aligning dark data governance with the organisation's business needs helps in ensuring that governance efforts are focused on areas that will drive the most value and support strategic goals (Lavallo and Smilde, 2021).
- **Integration of Dark Data with Business Strategy:** Aligning dark data governance with the organisation's business strategy ensures that dark data is leveraged to support business goals and drive value creation (Lavallo and Smilde, 2021).
- **Strategic Utilization of Data and Dark Data:** Develop strategies to utilize data and dark data effectively for business intelligence, innovation, and long-term business goals (Agrawal, 2019).

2. Business Scope, Data Scope, and Dark Data Classifications:

- **Data Stewardship:** Appointing data stewards ensures that data is managed effectively throughout its lifecycle, from creation to disposal, while maintaining its integrity within a defined business scope (DAMA, 2017).
- **Data Lifecycle Management:** Managing the data lifecycle as per business requirements from creation to retirement ensures that data remains relevant to business and compliant with regulatory requirements throughout its existence (HNU, 2020).

- **Data Classification Standards:** Establishing data classification standards helps in organizing data based on its sensitivity and value to business processes, ensuring that it is managed and protected appropriately (Weber, Otto, and Osterle, 2009).
- **Comprehensive Data Inventory:** Maintaining a comprehensive inventory of data assets helps in organizing, managing, and protecting data, which is essential for effective data governance that supports business operations (Collibra, 2020).
- **Identification of Dark Data Sources:** Identifying sources of dark data within the organisation is the first step in managing it effectively (Ajis and Baharin, 2019).
- **Classification of Dark Data:** Classifying dark data based on its sensitivity, value, and relevance to business helps in prioritizing data management efforts and ensuring that the most critical data is managed appropriately within the defined business scope. (Gartner, 2020).

3. Business Operations Compliance with Governance Policies, Standards, and Regulations

- **Regulatory Compliance:** Adhering to regulatory requirements not only ensures legal compliance but also protects the organisation from potential legal and financial penalties (Al-Ghamdi, Win, and Vlahu-Gjorgievska, 2020).
- **Privacy Management:** Implementing privacy management practices ensures that data governance activities comply with privacy laws and regulations, protecting individuals' data rights (Gallagher et al., 2015).
- **Compliance with Data Protection Laws:** Ensuring that dark data management practices by business operations comply with relevant data protection laws and regulations helps in mitigating legal risks across the organisation (Thiel, Stroetmann, and Singleton, 2014).
- **Dark Data Governance Compliance:** Conducting regular compliance audits for dark data ensures that governance practices implemented by business operations are aligned with legal requirements (Brous, Janssen, and Vilminko-Heikkinen, 2016).
- **Addressing Dark Data Privacy Concerns:** Implementing measures to address privacy concerns related to dark data helps in protecting individuals' data rights and ensuring compliance with privacy regulations (Thiel, Stroetmann, and Singleton, 2014).
- **Developing Dark Data Best Practices:** Establishing and promoting best practices by business operations for dark data governance helps in ensuring that this data is managed effectively, securely, and in alignment with industry standards (Lavalle and Smilde, 2021).
- **Dark Data Retention and Disposal Policies:** Developing and enforcing clear policies for the retention and disposal of dark data helps in managing storage costs, reducing risks, and ensuring compliance with regulatory requirements (Weber, Otto, and Osterle, 2009).
- **Mitigating Dark Data Legal Risks:** Developing strategies to mitigate legal risks associated with dark data, such as privacy violations or breaches of data protection laws, is crucial for protecting the organisation and ensure compliance (Thiel, Stroetmann, and Singleton, 2014).
- **Ethical Considerations in Dark Data Management:** Addressing ethical issues related to dark data, such as privacy concerns and data misuse, is crucial for maintaining trust and ensuring compliance with ethical standards (Thiel, Stroetmann, and Singleton, 2014).

1. Coordination, Collaboration, and Communication

- **Stakeholder Engagement:** Active involvement of stakeholders across all levels promotes buy-in and ensures that data governance initiatives are aligned with the needs and expectations of the business (Alreemy et al., 2016).

- Cross-functional Collaboration: Encouraging collaboration across different functions and departments enhances the effectiveness of data governance by ensuring that all perspectives and needs are considered (Alreemy et al., 2016).
- Data Governance Committee: Establishing a data governance committee function helps in overseeing data governance activities, ensuring alignment with business goals, and resolving any governance-related issues (Niemi, 2011).
- Effective Communication: Regular and transparent communication about data governance policies, roles, and expectations is vital for ensuring that all stakeholders are informed and engaged (Alreemy et al., 2016).
- Cross-Departmental Collaboration for Dark Data: Encouraging collaboration across departments ensures that dark data is managed consistently and effectively. Establishing cross-functional teams for dark data governance ensures that different perspectives and expertise are considered in the management of dark data (Ajis and Baharin, 2019).
- Effective Dark Data Communication: Developing a communication strategy for dark data governance ensures that all stakeholders are informed about policies, practices, and risks associated with dark data (Alreemy et al., 2016).
- Engagement with Regulatory Bodies: Actively engaging with regulatory bodies helps in staying informed about changes in regulations and ensuring that dark data governance practices remain compliant with current legal requirements (Thiel, Stroetmann, and Singleton, 2014).
- Legal Compliance Communication: Establishing clear channels for communicating legal compliance requirements across the organisation helps in ensuring that all stakeholders understand and adhere to relevant regulations (Thiel, Stroetmann, and Singleton, 2014).

2. Corporate Control, Cohesion, and Corporate Policy Development

- Data Access Control: Implementing robust common data access controls protects sensitive data from unauthorized access, ensuring data security and compliance with privacy regulations across the organisation to ensure cohesion (Gallaher et al., 2015).
- Corporate Data Ownership and Custodianship: Clearly defining ownership and custodianship corporate roles ensures that there is accountability for data across its lifecycle, enhancing data governance practices across the organisation (Weber, Otto, and Osterle, 2009).
- Incident Management and Response: Establishing incident management procedures helps in quickly addressing and controlling data governance breaches or issues, minimizing their impact on the organisation (Bruck, 2017).
- Data Policy Management: Effectively managing data policies ensures that they are up-to-date, aligned with business goals, and enforced consistently across the organisation, which is critical for successful data governance (Loshin, 2010).
- Policy Development and Enforcement: Developing and enforcing clear policies for data governance key domains: Data Architecture, Data Quality, Metadata, Data Security, Reference & Master Data, Data Warehousing/Business Intelligence/Artificial Intelligence, Data Modelling & Design, Document & Content Management, Data Storage & Infrastructure/Operation, Data Integration & Interoperability. This ensures consistent application of data management practices across the organisation. Also, documenting data governance processes helps in ensuring consistency, providing a reference for stakeholders, and supporting compliance with regulatory requirements at the corporate level. This ensures cohesion (Niemi, 2011), (DAMA, 2017).

- **Dark Data Quality Control:** Implementing policies and quality control measures for dark data ensures that it is accurate, consistent, and reliable, which is essential for its effective use in analytics and decision-making (Côrte-Real, Ruivo, and Oliveira, 2020).
- **Data Security in Dark Data Handling:** Implementing robust data security policies and measures for dark data helps in protecting it from unauthorized access, breaches, and other security threats (Al-Ghamdi, Win, and Vlahu-Gjorgievska, 2020).
- **Ensuring Data Accuracy and Relevance:** Implementing processes to ensure the accuracy and relevance of dark data helps in maximizing its value for business operations and ensuring that it supports informed decision-making (Côrte-Real, Ruivo, and Oliveira, 2020).
- **Metadata Management:** Effective metadata management helps in understanding the context, content, and structure of data, which is critical for data quality, retrieval, and governance (Otto, 2011).
- **Master Data Management (MDM):** Implementing MDM practices helps in maintaining consistent and accurate master data across the organisation, which is critical for effective data governance (Stedman and Vaughan, 2020).
- **Data Retention and Archiving Policies:** Developing clear policies for data retention and archiving ensures that data is stored appropriately and is accessible when needed, while also complying with regulatory requirements. Developing and enforcing retention policies for dark data ensures that it is stored for appropriate periods and disposed of when no longer needed by the business operations (Weber, Otto, and Osterle, 2009).
- **Developing Dark Data Governance Policies:** Establishing clear policies for the governance of dark data ensures that it is managed consistently and effectively across the organisation. Developing a comprehensive framework for the governance of dark data ensures that it is managed systematically and consistently across the organisation (Gartner, 2020).
- **Automation of Dark Data Governance Processes:** Implementing automation in dark data governance processes helps in reducing manual effort, increasing efficiency, and ensuring consistency (Lavalle and Smilde, 2021).
- **Resource Allocation for Data Governance:** Allocating sufficient resources to data governance initiatives at corporate level ensures that they are effectively implemented and sustained over time (Niemi, 2011).
- **Support from Executive Leadership:** Securing support from executive leadership is crucial for the success of corporate data governance initiatives. This helps in securing resources, driving adoption, and aligning governance with business goals to ensure cohesion (Weber, Otto, and Osterle, 2009).
- **Resource Allocation for Dark Data Management:** Allocating sufficient resources for dark data management ensures that the organisation can effectively control and manage this data, including storage, processing, and analysis (Sun, Su, and Shen, 2023).
- **Establishing Dark Data Governance Roles:** Defining specific roles and responsibilities for dark data governance ensures that this data is managed effectively and that there is accountability at every stage. Setting up a dedicated office for dark data governance helps in centralizing governance efforts, ensuring consistency, and providing a focal point for managing dark data (DAMA, 2017).

6. Audit and Monitoring

- Continuous Monitoring and Auditing: Regular monitoring and auditing of data governance processes ensure that they remain effective and compliant with internal and external standards (Brous, Janssen, and Vilminko-Heikkinen, 2016).
- Data Protection Impact Assessments: Conducting regular data protection impact assessments helps in identifying potential risks to data privacy and security, ensuring compliance with regulatory requirements (Thiel, Stroetmann, and Singleton, 2014).
- Auditable Data Governance Processes: Ensuring that data governance processes are auditable helps in demonstrating compliance with internal and external standards, which is essential for maintaining trust and accountability (Brous, Janssen, and Vilminko-Heikkinen, 2016).
- Vendor and Third-Party Data Governance: Ensuring that vendors and third parties comply with the organisation's data governance policies helps in protecting data across the entire supply chain and reducing risks associated with external partnerships (Al-Ruithe, Benkhelifa, and Hameed, 2018).
- Dark Data Audit Trails: Establishing audit trails for dark data helps in tracking how this data is accessed, used, and managed, which is essential for ensuring compliance and accountability (Brous, Janssen, and Vilminko-Heikkinen, 2016).
- Regular Dark Data Policy Reviews: Conducting regular reviews of dark data governance policies helps in ensuring that they remain up-to-date, relevant, and effective in the face of changing regulations, technologies, and business needs (Weber, Otto, and Osterle, 2009).
- Monitoring Dark Data Governance Effectiveness: Regularly monitoring and assessing the effectiveness of dark data governance practices helps in identifying areas for improvement and ensuring that governance initiatives remain aligned with organisational goals (Curtiss, Saxena, and Seth, 2018).
- Dark Data Governance Metrics and KPIs: Defining and tracking metrics and KPIs for dark data governance helps in measuring the effectiveness of governance efforts and identifying areas for improvement (Curtiss, Saxena, and Seth, 2018).

7. Adaptation, Agility, and Learning

- Adaptation to Environmental Changes: Organisations must be agile and responsive to changes in the external environment, including new regulations, emerging technologies, and shifting market dynamics, to sustain their data governance initiatives (Brous, Janssen, and Vilminko-Heikkinen, 2016).
- Adoption of Industry Best Practices: Adopting best practices from industry leaders helps in ensuring that data governance practices are effective, efficient, and aligned with global standards (DAMA, 2017).
- Proactive Data Governance: Taking a proactive approach to managing risks associated with data governance helps in preventing potential issues and ensuring the resilience of governance practices (Al-Ghamdi, Win, and Vlahu-Gjorgievska, 2020).
- Agile Governance: Implementing governance structures that are agile and responsive to changes in the data environment, ensuring adaptability and resilience. Developing a long-term strategy for managing dark data helps in ensuring that governance practices are sustainable and adaptable to future changes in the data landscape in alignment with the organisation's future goals. Regular Dark Data Policy Reviews help in ensuring that they remain up-to-date, relevant, and effective in the face of changing regulations, technologies, and business needs (Weber, Otto, and Osterle, 2009).
- Agility in Data Governance: Implementing agile data governance practices allows organisations to quickly adapt to changes in the data landscape, ensuring that governance practices remain relevant and effective (Baškarada, Gao, and Koronios,

2006). Implementing agile governance practices for dark data allows organisations to quickly adapt to changes in the data landscape (Lavallo and Smilde, 2021).

- **Effective Data Governance Leadership:** Strong leadership in data governance helps in driving governance initiatives, securing resources, and ensuring alignment with long-term organisational goals to support adaptation (DAMA, 2017).
- **Alignment with Organisational Strategic Goals:** Ensuring that dark data governance is aligned with the organisation's overall objectives helps in maximizing the value of this data and ensuring that it supports strategic goals (Lavallo and Smilde, 2021).
- **Adaptation to Environmental Changes:** Organisations must be agile and responsive to changes in the external environment, including new regulations, emerging technologies, and shifting market dynamics (Sun, Su, and Shen, 2023).
- **Leveraging Dark Data for Competitive Advantage:** Developing strategies to leverage dark data for competitive advantage helps in unlocking its value, identifying new opportunities, and differentiating the organisation in the market (Agrawal, 2019).
- **Proactive Risk Management in Dark Data Initiatives:** Developing and implementing risk management strategies for dark data initiatives helps in adaptation, identifying and mitigating potential risks (Sun, Su, and Shen, 2023).

8. Integrated Governance

- **Integration with IT Governance:** Aligning data governance with IT governance ensures that data management practices are integrated with the organisation's IT infrastructure and processes, leading to more efficient and effective governance (Alreemy et al., 2016).
- **Data Integration and Interoperability:** Ensuring that data governance practices facilitate the integration and interoperability of data across different systems and platforms enhances data usability and governance (Otto, 2011).
- **Integration of Data Governance in Cloud Environments:** Adapting data governance practices for cloud environments ensures that data remains secure and compliant when stored or processed in the cloud (Al-Ruithe, Benkhelifa, and Hameed, 2018).
- **Integration with Enterprise Architecture:** Aligning data governance with enterprise architecture ensures that data management practices are integrated into the broader IT and business infrastructure, enhancing overall governance (Guetat and Dakhli, 2015).
- **Data Governance for Data Analytics:** Implementing data governance practices tailored to data analytics high-tech initiatives ensures that data used for analytics is accurate, consistent, and secure, supporting better decision-making (Côte-Real, Ruivo, and Oliveira, 2020).
- **Effective Governance of Big Data Initiatives:** Implementing data governance practices tailored to big data high-tech initiatives ensures that large and complex datasets are managed effectively and securely (Côte-Real, Ruivo, and Oliveira, 2020).
- **Integration of Dark Data into Big Data Analytics:** Ensuring that dark data is integrated into big data analytics high-tech initiatives helps in maximizing the value of all available data and supporting more comprehensive analytics and insights (Lavallo and Smilde, 2021).
- **Integration with Corporate Strategy:** Aligning dark data governance with the organisation's corporate strategy ensures that governance efforts are focused on areas that will drive the most value and support long-term business objectives (Lavallo and Smilde, 2021).
- **Integration with IT Infrastructure:** Ensuring that dark data governance practices are integrated with the organisation's IT infrastructure helps in streamlining data management processes and ensuring consistency across the organisation (Weber, Otto, and Osterle, 2009).

- Integration with Existing Data Governance: Integrating dark data governance with the organisation's existing data governance framework ensures consistency and avoids duplication of efforts (Lavalle and Smilde, 2021).
- Dark Data Governance in Cloud Environments: Adapting dark data governance practices for cloud environments helps in ensuring that dark data stored or processed in the cloud is secure, compliant, and effectively managed (Al-Ruithe, Benkhelifa, and Hameed, 2018).

9. Corporate Metadata Management and Common Understanding

- Metadata Management: Effective metadata management is essential for understanding the context, content, and structure of data, including dark data classification, to ensure common understanding (Otto, 2011).
- Standardized Data Definitions: Establish standardized definitions for key data elements to ensure a common understanding across the organisation, facilitating consistent governance practices (Weber, Otto, and Osterle, 2009).
- Common Understanding through Metadata: Use metadata to foster a shared understanding of data across the organisation, reducing the risks of misinterpretation and ensuring better data integration (Koooper, Maes, and Lindgreen, 2011).

10. Training and Change Management

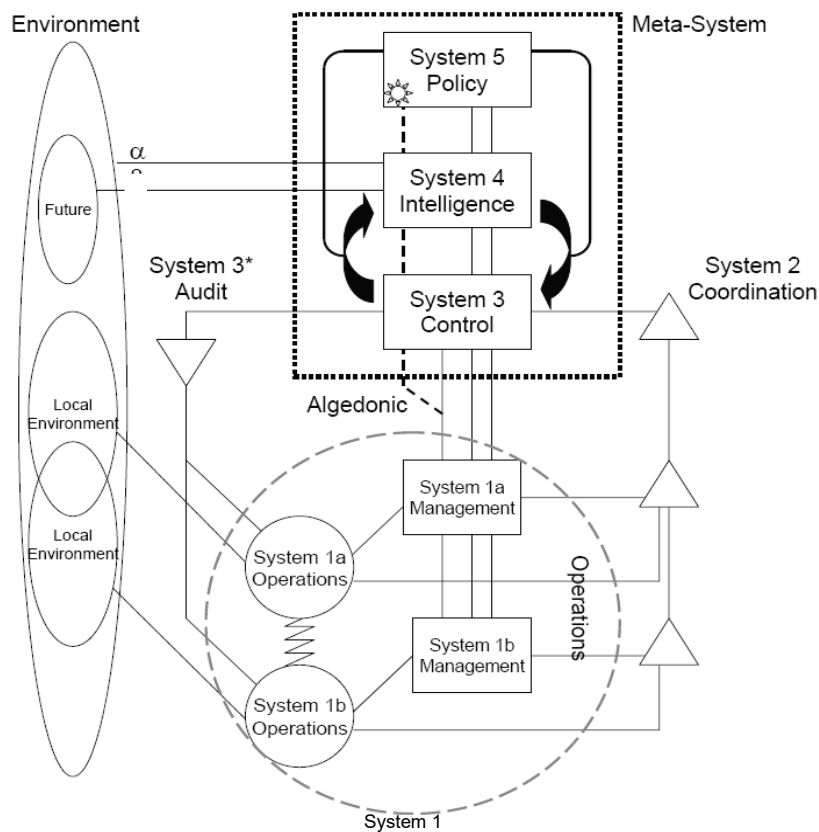
- Change Management: Successfully managing changes in data governance practices involves preparing, supporting, and helping individuals, teams, and the organisation to adapt to changes (Mento, 2002).
- Effective Data Stakeholders Training: Providing training for data stakeholders ensures that they have the skills and knowledge needed to manage data effectively, which is essential for effectively implementing data governance functions. Providing regular training on dark data governance helps in ensuring that employees are aware of the latest practices, technologies, and regulations related to dark data (DAMA, 2017).
- Creating Dark Data Awareness Programs: Developing and implementing awareness programs on dark data helps in educating employees about the importance of managing and protecting dark data (DAMA, 2017).
- Cross-functional Dark Data Governance Teams: Establishing cross-functional teams for dark data governance ensures that different perspectives and expertise are considered in the management of dark data (Ajis and Baharin, 2019).
- Transparent Dark Data Practices: Promoting transparency in dark data management practices helps in building trust with stakeholders and ensuring that the organisation's data governance activities are understood and supported (Lavalle and Smilde, 2021).
- Creating a Culture of Dark Data Awareness: Promoting a culture of awareness around dark data helps in ensuring that all employees understand the importance of managing and protecting this data (Weber, Otto, and Osterle, 2009).

11. Continuous Improvements and Maturity Models

- Continuous Improvement of Data and Dark Data Practices: Regular monitoring and auditing of data governance processes ensure that they remain effective and compliant with internal and external standards. This ensures continuous improvements. Establishing a process for continuous improvement in dark data governance helps in ensuring that governance practices are regularly evaluated and enhanced based on lessons learned and evolving needs (Brous, Janssen, and Vilminko-Heikkinen, 2016).
- Dark Data Governance Metrics and KPIs: Defining and tracking key performance indicators (KPIs) for data governance allows organisations to measure the effectiveness of their governance initiatives and make informed improvements (Curtiss, Saxena, and Seth, 2018).

- **Monitoring Data Governance Effectiveness:** Regularly monitoring and assessing the effectiveness of data governance practices helps in identifying areas for improvement and ensuring that governance initiatives are continuously improved to remain aligned with organisational goals (Curtiss, Saxena, and Seth, 2018).
- **Continuous Improvements for Data Governance:** Establishing a process for ongoing evaluation and improvement of data governance practices ensures that they remain relevant and effective (Brous, Janssen, and Vilminko-Heikkinen, 2016).
- **Data Governance Maturity Model Assessment:** Regularly assessing the maturity of data governance practices helps organisations understand their current state and identify areas for improvement (HNU, 2020).
- **Continuous Monitoring of Dark Data:** Regular monitoring of dark data helps in identifying new sources of dark data and ensuring that it is managed effectively over time (Wiebe and Allison, 2015).
- **Understanding the Value of Dark Data:** Conducting assessments to understand the potential value of dark data helps in prioritizing data management efforts and ensuring that valuable insights are not overlooked (Lavalle and Smilde, 2021).

Appendix H: The Viable System Model's Symbols (Adapted from Beer, 1985)



The symbols in the Viable System Model (VSM) have specific meanings.

- The large ellipse to the left represents the environment in which the organisation is immersed.
- The squares represent Management Functions
- The two circles and the attached squares represent operations and their local management functions respectively. System 1 of the system-in-focus is the collection of these operational elements.
- The small ellipses represent the "local" environments relevant to the operational elements.
- Triangles represent Coordination or Audit Functions
- The remaining squares and triangles represent Systems 2 to 5, as indicated by the labels in the above VSM Figure.
- System 3, System 4, and System 5 represent the Meta-System (Senior Management/ leadership).
- The lines between the symbols indicate communication channels
- Data/information domains are the key data flows within and across the five VSM System.

Appendix I: Data Governance Domains - Key Descriptions

(Weill, P. and Ross, W. J., 2004):

Key descriptions for: Data Architecture, Data Quality, Metadata, Data Security, Reference & Master Data, Data Warehousing/Business Intelligence/Artificial Intelligence, Data Modelling & Design, Document & Content Management, Data Storage & Infrastructure/Operation, Data Integration & Interoperability:

1. **Data Architecture:** Data architecture defines the structure, storage, and movement of data within an organisation. It includes the design and management of data models, databases, data warehouses, and data integration processes. The aim is to ensure that data is organised and accessible. Reference: Inmon, W.H., 2005. *Building the Data Warehouse*. 4th ed. John Wiley & Sons.
2. **Data Quality:** Data quality ensures that data is accurate, complete, reliable, and relevant. It involves processes for data cleansing, validation, and enrichment to maintain high standards of data. Reference: Redman, T.C., 2017. *Data Driven: Profiting from Your Most Important Business Asset*. Harvard Business Review Press.
3. **Metadata:** Metadata management involves the creation, organisation, and control of metadata, which is data about data. It helps in understanding the data's source, structure, and usage. Reference: Marco, D., 2000. *Building and Managing the Meta Data Repository: A Full Lifecycle Guide*. Wiley.
4. **Data Security:** Data security ensures the protection of data from unauthorized access and breaches. It includes encryption, access controls, and compliance with regulations to safeguard sensitive information. Reference: Shon Harris, 2013. *CISSP All-in-One Exam Guide*. 6th ed. McGraw-Hill.
5. **Reference & Master Data:** Reference and master data management (RDM/MDM) involves the consistent and accurate management of critical data across the organisation. This ensures a single version of the truth for key business entities. Reference: Loshin, D., 2011. *Master Data Management*. Morgan Kaufmann.
6. **Data Warehousing/Business Intelligence/Artificial Intelligence:** This domain covers the storage of large volumes of data (data warehousing), and the analysis of this data for business insights (business intelligence). Artificial intelligence (AI) is increasingly used to enhance these processes. Reference: Kimball, R., Ross, M., 2013. *The Data Warehouse Toolkit: The Definitive Guide to Dimensional Modelling*. 3rd ed. Wiley.
7. **Data Modelling & Design:** Data modelling and design involve creating models that define the structure, relationships, and constraints of data. This helps in the effective organisation and use of data. Reference: Simsion, G.C., Witt, G.C., 2004. *Data Modelling Essentials*. 3rd ed. Morgan Kaufmann.
8. **Document & Content Management:** This domain manages the lifecycle of documents and content within the organisation, ensuring they are stored, retrieved, and disposed of effectively. Reference: Smith, H.A., McKeen, J.D., 2003. *Developments in Practice XXX: Creating and Sustaining a Superior Enterprise Content Management (ECM) Capability*. Communications of the Association for Information Systems, 11(1), pp. 1-27.
9. **Data Storage & Infrastructure/Operation:** This involves physical and virtual storage solutions for data, including data centres, cloud storage, and database management systems. It ensures data availability, reliability, and performance. Reference: Silberschatz, A., Korth, H.F., Sudarshan, S., 2010. *Database System Concepts*. 6th ed. McGraw-Hill.
10. **Data Integration & Interoperability:** Data integration involves combining data from different sources to provide a unified view, while interoperability ensures that different

systems can work together seamlessly. Reference: Wrembel, R., 2011. *Data Warehouses and OLAP: Concepts, Architectures, and Solutions*. IGI Global.

These domains collectively ensure comprehensive data governance, facilitating effective data management and utilization across organisations.

Appendix J: VSM Qualities vs. Assessment of Different Key Governance Models

Appendix J.1: VSM Qualities vs. Assessment of Different Governance Models

This Appendix provides a comparison of the various governance models for the key researchers: [\(Young, D., 1996\)](#), [\(Jessop, B., 1998\)](#), [\(Rosenau, N, J., 1992\)](#), [\(Carver, J., 1997\)](#), [\(Charkham, J., 1994\)](#), [\(Kay, J. and Silbertson, A., 1995\)](#) against the key qualities of Beer's Viable Systems Model (VSM). Each model has strengths and weaknesses in addressing these qualities, which helps in understanding the extent to which they support organisational viability and effectiveness.

VSM Key Systemic Function	Young's Feedback Model	Jessop's Coordination Model	Rosenau's Comprehensive Model	Carver's Policy Governance Model	Charkham's Accountability Model	Kay et al.'s Trusteeship Model	VSM Model (Beer)
S1: Operational Units	Implied but not explicitly detailed	Implied but not explicitly detailed	Detailed, but lacks operational execution	Lacks detailed mechanisms for operational execution	Not explicitly detailed	Lacks detailed operational mechanisms	Provides a clear structure for operational units as autonomous sub-systems
S2: Coordination	Not explicitly addressed	Emphasizes coordination	Conceptual but lacks operational mechanisms	Implied but not explicitly detailed	Implied but not explicitly detailed	Not explicitly detailed	Ensures coordination of autonomous units to prevent conflicts
S3: Control	Implied through feedback mechanisms	Implied through coordination	Conceptual but lacks detailed control mechanisms	Focuses on values and strategic alignment, lacks detailed control	Emphasizes accountability but lacks strategic control mechanisms	Focuses on values and identity, lacks detailed control mechanisms	Includes operational planning, monitoring, and control

VSM Key Systemic Function	Young's Feedback Model	Jessop's Coordination Model	Rosenau's Comprehensive Model	Carver's Policy Governance Model	Charkham's Accountability Model	Kay et al.'s Trusteeship Model	VSM Model (Beer)
S3*: Audit	Not explicitly addressed	Not explicitly addressed	Conceptual but lacks detailed auditing mechanisms	Not explicitly addressed	Emphasizes accountability but lacks independent audit mechanisms	Not explicitly addressed	Provides independent audit and monitoring functions
S4: Intelligence	Implied through feedback and learning mechanisms	Implies strategic flexibility and responsiveness	Comprehensive strategic development	Emphasizes strategic thinking and long-term planning	Implies strategic adaptation but lacks detailed intelligence	Emphasizes values and strategic thinking	Focuses on intelligence and strategy development
S5: Identity and Policy	Implied through feedback and organizational alignment	Implies building shared values and identity	Comprehensive identity and vision development	Strong focus on identity, vision, and values	Emphasizes balancing power and accountability	Strong focus on identity and values	Emphasizes identity, vision, and policy development
Requisite Variety	Implied but not explicitly detailed	Implies necessary coordination and adaptation	Comprehensive but lacks detailed mechanisms	Implies adaptability but lacks explicit mechanisms	Implies necessary balance but lacks explicit mechanisms	Implies balance and adaptability	Ensures requisite variety to manage complexity
Communication Channels	Lacks differentiation of horizontal and vertical channels	Implies coordination but lacks emphasis on information flows	Comprehensive but lacks detailed communication channels	Implies communication for strategic alignment	Emphasizes checks and balances but lacks detailed channels	Implies communication but lacks detailed channels	Emphasizes clear communication and feedback channels

VSM Key Systemic Function	Young's Feedback Model	Jessop's Coordination Model	Rosenau's Comprehensive Model	Carver's Policy Governance Model	Charkham's Accountability Model	Kay et al.'s Trusteeship Model	VSM Model (Beer)
Adaptability and Learning	Emphasizes feedback and learning mechanisms	Implies adaptability through coordination	Comprehensive but lacks detailed adaptability mechanisms	Emphasizes strategic adaptation and learning	Implies adaptability but lacks detailed mechanisms	Implies adaptability but lacks detailed mechanisms	Focuses on adaptability and continuous learning
Balance of Autonomy and Control	Not explicitly addressed	Emphasizes coordination, lacks detailed control	Comprehensive balance but lacks operational mechanisms	Emphasizes values and strategic alignment, lacks detailed control	Emphasizes balancing power and accountability	Implies balance but lacks detailed control mechanisms	Ensures balance between autonomy and control
Integration of Sub-Systems	Lacks comprehensive integration	Implies integration through coordination	Comprehensive but lacks detailed integration mechanisms	Emphasizes strategic alignment and values	Implies integration but lacks detailed mechanisms	Implies integration but lacks detailed mechanisms	Integrates all sub-systems for organisational coherence
Recursivity	Not explicitly addressed	Not explicitly addressed	Conceptual but lacks detailed recursive structures	Implied but not explicitly detailed	Implied but not explicitly detailed	Not explicitly addressed	Emphasizes recursive structures, where each sub-system contains all VSM functions
Transduction	Not explicitly addressed	Not explicitly addressed	Conceptual but lacks detailed transduction	Implied but not explicitly detailed	Implied but not explicitly detailed	Not explicitly addressed	Emphasizes transduction, ensuring accurate transmission

VSM Key Systemic Function	Young's Feedback Model	Jessop's Coordination Model	Rosenau's Comprehensive Model	Carver's Policy Governance Model	Charkham's Accountability Model	Kay et al.'s Trustship Model	VSM Model (Beer)
			mechanisms				and transformation of information across systems
Algedonic Channels	Not explicitly addressed	Not explicitly addressed	Conceptual but lacks detailed algedonic channels	Implied but not explicitly detailed	Implied but not explicitly detailed	Not explicitly addressed	Includes algedonic channels for handling critical alerts and deviations

Appendix J.2: VSM Qualities vs. Assessment of existing Governance Models (Key researchers)

This Appendix provides a comparison of the key data governance models proposed by the key researchers: ([\(Khatri, V. and Brown, C., 2010\)](#)), ([\(Otto, B., 2011\)](#)), ([\(Weber, K., Otto, B. and Osterle, H., 2009\)](#)), ([\(Ajis, M, F, A. and Baharin, H, S., 2019\)](#)), ([\(Huygh, T. and Haes, D, S., 2018\)\)](#) against the key qualities of VSM. Each model has strengths and weaknesses in addressing these qualities, which helps in understanding the extent to which they support organisational viability and effectiveness.

VSM Quality	Designing Data Governance (Khatri & Brown, 2010)	A Morphology of the Organisation of Data Governance (Otto, 2011)	One Size Does Not Fit All: A Contingency Approach to Data Governance	Dark Data Management as Frontier of Information Governance	Using the Viable System Model to Study IT Governance Dynamics	VSM Model (Beer, 1981)
S1: Operational Units	Implies detailed processes and practices for data management	Describes roles and responsibilities in data governance	Emphasizes the contingency approach for data governance	Addresses operational units through dark data management principles	Focuses on IT governance dynamics	Provides clear structure for operational units as autonomous sub-systems

VSM Quality	Designing Data Governance (Khatr & Brown, 2010)	A Morphology of the Organisation of Data Governance (Otto, 2011)	One Size Does Not Fit All: A Contingency Approach to Data Governance	Dark Data Management as Frontier of Information Governance	Using the Viable System Model to Study IT Governance Dynamics	VSM Model (Beer, 1981)
S2: Coordination	Emphasizes coordination between data and business objectives	Describes coordination of decision rights	Emphasizes coordination based on organisational needs	Coordination through compliance and regulatory requirements	Emphasizes coordination within IT governance	Ensures coordination of autonomous units to prevent conflicts
S3: Control	Includes detailed control objectives and audit guidelines	Describes control mechanisms for data quality	Focuses on establishing control based on contingency	Includes control through dark data management strategies	Emphasizes control mechanisms in IT governance	Includes operational planning, monitoring, and control
S3*: Audit	Provides specific audit guidelines and frameworks	Describes audit roles in data governance	Conceptual but includes audit mechanisms	Emphasizes mandatory audits for dark data	Includes audit mechanisms within IT governance	Provides independent audit and monitoring functions
S4: Intelligence	Focuses on aligning data strategy with business strategy	Describes strategic intelligence roles in data governance	Emphasizes intelligence based on organisational needs	Emphasizes strategic intelligence for dark data management	Focuses on strategic intelligence in IT governance	Focuses on intelligence and strategy development
S5: Identity and Policy	Provides a framework for data governance policies	Emphasizes establishing identity and policy roles	Focuses on identity and policy based on contingency	Emphasizes identity and policy for dark data management	Establishes identity and policy in IT governance	Emphasizes identity, vision, and policy development
Requisite Variety	Ensures variety through detailed data governance practices	Emphasizes adaptability through comprehensive data governance	Lacks explicit mechanisms for requisite variety	Ensures variety through dark data management practices	Ensures requisite variety through IT governance	Ensures requisite variety to manage complexity

VSM Quality	Designing Data Governance (Khatri & Brown, 2010)	A Morphology of the Organisation of Data Governance (Otto, 2011)	One Size Does Not Fit All: A Contingency Approach to Data Governance	Dark Data Management as Frontier of Information Governance	Using the Viable System Model to Study IT Governance Dynamics	VSM Model (Beer, 1981)
Communication Channels	Includes frameworks for communication between data and business	Emphasizes communication across data governance roles	Lacks detailed communication channels	Ensures communication for dark data management	Emphasizes communication channels in IT governance	Emphasizes clear communication and feedback channels
Adaptability and Learning	Emphasizes continuous improvement and learning	Focuses on continuous learning in data governance	Implies adaptability but lacks detailed mechanisms	Ensures adaptability through dark data management measures	Focuses on continuous learning in IT governance	Focuses on adaptability and continuous learning
Balance of Autonomy and Control	Ensures balance through defined data governance practices	Emphasizes balance through roles and responsibilities	Implied but lacks detailed mechanisms for balance	Ensures balance through dark data management strategies	Emphasizes balance in IT governance	Ensures balance between autonomy and control
Integration of Sub-Systems	Ensures integration through comprehensive data governance frameworks	Emphasizes integration across data governance roles	Conceptual but lacks detailed integration mechanisms	Ensures integration through dark data management measures	Focuses on integration in IT governance	Integrates all sub-systems for organisational coherence
Recursivity	Not explicitly addressed	Not explicitly addressed	Conceptual but lacks detailed recursive structures	Implied but not explicitly detailed	Emphasizes recursive structures in IT governance	Emphasizes recursive structures, where each sub-system contains all VSM functions
Transduction	Not explicitly addressed	Not explicitly addressed	Conceptual but lacks detailed transduction	Implied but not explicitly detailed	Implied but not explicitly detailed	Emphasizes transduction, ensuring accurate

VSM Quality	Designing Data Governance (Khatri & Brown, 2010)	A Morphology of the Organisation of Data Governance (Otto, 2011)	One Size Does Not Fit All: A Contingency Approach to Data Governance	Dark Data Management as Frontier of Information Governance	Using the Viable System Model to Study IT Governance Dynamics	VSM Model (Beer, 1981)
			n mechanisms			transmission and transformation of information across systems
Algedonic Channels	Not explicitly addressed	Not explicitly addressed	Conceptual but lacks detailed algedonic channels	Implied but not explicitly detailed	Implied but not explicitly detailed	Includes algedonic channels for handling critical alerts and deviations

Appendix K: VSM Qualities vs. Assessment of Key Industry Governance Models

By using the qualities of VSM for assessment, one can determine the strengths and weaknesses of different governance models and how well they support the viability and effectiveness of an organisation.

This Appendix provides a comparison of the following key industry governance models against the key qualities of VSM:

- COBIT (Control Objectives for Information and Related Technologies) ISACA, 2012
- DAMA-DMBOK (Data Management Body of Knowledge): DAMA International, 2017
- ISO/IEC 38500 (Corporate Governance of Information Technology): ISO, 2015.
- GDPR (General Data Protection Regulation): European Union, 2016
- CDMC (Cloud Data Management Capabilities): EDM Council, 2021

Each model has strengths and weaknesses in addressing these qualities, which helps in understanding the extent to which they support organisational viability and effectiveness.

VSM Quality	COBIT (Control Objectives for Information and Related Technologies)	DAMA-DMBOK (Data Management Body of Knowledge)	ISO/IEC 38500 (Corporate Governance of Information Technology)	GDPR (General Data Protection Regulation)	CDMC (Cloud Data Management Capabilities)	VSM Model (Beer)
S1: Operational Units	Provides detailed processes and practices for IT management (ISACA, 2012)	Defines data management functions and activities (DAMA, 2017)	Implied through governance practices but lacks operational execution (ISO, 2015)	Operational units addressed through data protection principles (EU, 2016)	Focuses on capabilities in cloud data management (EDM Council, 2021)	Provides clear structure for operational units as autonomous sub-systems
S2: Coordination	Emphasizes coordination between IT and business objectives (ISACA, 2012)	Coordination across data management disciplines (DAMA, 2017)	Emphasizes strategic alignment but lacks detailed coordination mechanism	Coordination through compliance and regulatory requirements (EU, 2016)	Emphasizes coordination of cloud data capabilities (EDM Council, 2021)	Ensures coordination of autonomous units to prevent conflicts

VSM Quality	COBIT (Control Objectives for Information and Related Technologies)	DAMA-DMBOK (Data Management Body of Knowledge)	ISO/IEC 38500 (Corporate Governance of Information Technology)	GDPR (General Data Protection Regulation)	CDMC (Cloud Data Management Capabilities)	VSM Model (Beer)
			s (ISO, 2015)			
S3: Control	Includes detailed control objectives and audit guidelines (ISACA, 2012)	Focuses on data governance and stewardship (DAMA, 2017)	Implies control mechanisms but lacks detailed guidelines (ISO, 2015)	Includes control through data protection impact assessments (EU, 2016)	Emphasizes control through capability assessments (EDM Council, 2021)	Includes operational planning, monitoring, and control
S3*: Audit	Provides specific audit guidelines and frameworks (ISACA, 2012)	Emphasizes auditing and monitoring within data governance (DAMA, 2017)	Conceptual but lacks detailed auditing mechanisms (ISO, 2015)	Includes mandatory audits for compliance (EU, 2016)	Focuses on auditing cloud data management capabilities (EDM Council, 2021)	Provides independent audit and monitoring functions
S4: Intelligence	Focuses on aligning IT strategy with business strategy (ISACA, 2012)	Emphasizes strategic data management and planning (DAMA, 2017)	Includes strategic alignment but lacks detailed intelligence mechanisms (ISO, 2015)	Emphasizes data protection by design and by default (EU, 2016)	Utilizes data intelligence for cloud data management (EDM Council, 2021)	Focuses on intelligence and strategy development
S5: Identity and Policy	Provides a framework for IT governance policies (ISACA, 2012)	Emphasizes establishing data governance policies and standards (DAMA, 2017)	Focuses on governance principles but lacks detailed identity mechanisms (ISO, 2015)	Emphasizes the creation of data protection policies (EU, 2016)	Establishes policies for cloud data governance (EDM Council, 2021)	Emphasizes identity, vision, and policy development
Requisite Variety	Ensures variety	Emphasizes adaptability	Lacks explicit	Ensures variety	Ensures requisite	Ensures requisite

VSM Quality	COBIT (Control Objectives for Information and Related Technologies)	DAMA-DMBOK (Data Management Body of Knowledge)	ISO/IEC 38500 (Corporate Governance of Information Technology)	GDPR (General Data Protection Regulation)	CDMC (Cloud Data Management Capabilities)	VSM Model (Beer)
	through detailed control objectives (ISACA, 2012)	through comprehensive data management practices (DAMA, 2017)	mechanisms for requisite variety (ISO, 2015)	through adaptable data protection measures (EU, 2016)	variety through cloud data capabilities (EDM Council, 2021)	variety to manage complexity
Communication Channels	Includes frameworks for communication between IT and business (ISACA, 2012)	Emphasizes communication across data management functions (DAMA, 2017)	Lacks detailed communication channels (ISO, 2015)	Ensures communication for compliance and accountability (EU, 2016)	Emphasizes communication channels for cloud data governance (EDM Council, 2021)	Emphasizes clear communication and feedback channels
Adaptability and Learning	Emphasizes continuous improvement and learning (ISACA, 2012)	Focuses on continuous learning and improvement in data management (DAMA, 2017)	Implies adaptability but lacks detailed mechanisms (ISO, 2015)	Ensures adaptability through continuous data protection measures (EU, 2016)	Focuses on continuous improvement of cloud data capabilities (EDM Council, 2021)	Focuses on adaptability and continuous learning
Balance of Autonomy and Control	Ensures balance through defined control objectives (ISACA, 2012)	Emphasizes balance through data stewardship practices (DAMA, 2017)	Implied but lacks detailed mechanisms for balance (ISO, 2015)	Ensures balance through data protection policies and controls (EU, 2016)	Emphasizes balance of autonomy and control in cloud data management (EDM Council, 2021)	Ensures balance between autonomy and control
Integration of Sub-Systems	Ensures integration through	Emphasizes integration across data	Conceptual but lacks detailed	Ensures integration through	Focuses on integration of cloud	Integrates all sub-systems for

VSM Quality	COBIT (Control Objectives for Information and Related Technologies)	DAMA-DMBOK (Data Management Body of Knowledge)	ISO/IEC 38500 (Corporate Governance of Information Technology)	GDPR (General Data Protection Regulation)	CDMC (Cloud Data Management Capabilities)	VSM Model (Beer)
	comprehensive IT governance frameworks (ISACA, 2012)	management domains (DAMA, 2017)	integration mechanisms (ISO, 2015)	comprehensive data protection measures (EU, 2016)	data management capabilities (EDM Council, 2021)	organisational coherence
Recursivity	Not explicitly addressed	Not explicitly addressed	Conceptual but lacks detailed recursive structures (ISO, 2015)	Implied but not explicitly detailed (EU, 2016)	Implied but not explicitly detailed (EDM Council, 2021)	Emphasizes recursive structures, where each sub-system contains all VSM functions
Transduction	Not explicitly addressed	Not explicitly addressed	Conceptual but lacks detailed transduction mechanisms (ISO, 2015)	Implied but not explicitly detailed (EU, 2016)	Implied but not explicitly detailed (EDM Council, 2021)	Emphasizes transduction, ensuring accurate transmission and transformation of information across systems
Algedonic Channels	Not explicitly addressed	Not explicitly addressed	Conceptual but lacks detailed algedonic channels (ISO, 2015)	Implied but not explicitly detailed (EU, 2016)	Implied but not explicitly detailed (EDM Council, 2021)	Includes algedonic channels for handling critical alerts and deviations

Appendix L: The Methodology of Diagnosis and Design by VSM

Quality Checklist for Existence and Quality of VSM 5 Systems (Jackson, M., 2003):

System 1:

1. For each part of System 1, detail its environment, operations, and localized management.
2. Ensure that each part of System 1 has the capacity to be viable in its own right.
3. Study what constraints are imposed upon the parts of System 1 by higher management.
4. Ask how accountability is exercised for each part and what indicators of performance are used.
5. Model System 1 according to the VSM diagram.

System 2:

1. List possible sources of disturbance or conflict in the organisation.
2. Identify various elements of System 2 that are needed to ensure harmonization and coordination.
3. Ask how System 2 is perceived in the organisation: threatening or facilitating.

System 3:

1. List System 3 activities of the system in focus.
2. Ask how System 3 exercises authority - is this seen as autocratic or democratic in System 1 and how much freedom do System 1 elements possess?
3. Assess how good System 3 is at translating overall policy into operational plans.
4. Evaluate how the 'resource bargain' with the parts of System 1 is carried out.
5. Ensure all control activities clearly facilitate the achievement of purpose.
6. Measure the performance of System 3 elements in enabling achievement of the purpose.

System 3*

1. Identify who can oversee the performance of the parts of System 1.
2. Evaluate what audit inquiries into aspects of System 1 System 3 conducts and whether these are appropriate.

System 4:

1. List all System 4 activities of the system in focus.
2. Assess how far ahead these activities consider.
3. Ensure these activities guarantee adaptation to the future.
4. Confirm that System 4 is monitoring what is happening in the environment and assessing the trends.
5. Determine if System 4 is open to novelty.
6. Ensure System 4 provides a management centre/operations room, bringing together external and internal information and providing an 'environment for decision'.
7. Verify that System 4 adequately processes, filters, and distributes relevant information.
8. Ensure all development activities clearly facilitate the achievement of purpose.
9. Measure the performance of System 4 elements in enabling achievement of the purpose.

System 5:

1. Identify who is responsible for policy (e.g., on the 'board') and how they act.
2. Ensure System 5 provides a suitable identity and conveys clear purposes for the system in focus.
3. Assess how the 'ethos' set by System 5 affects the perception of System 4.
4. Evaluate how the 'ethos' set by System 5 affects the relationship between Systems 3 and 4 - is stability or change emphasized?

5. Ensure System 5 is organised to behave creatively.
6. Verify if System 5 shares an identity with System 1 or claims to be something different.

Appendix M: Literature Review of HDG - Maturity Model (HDG-MM)

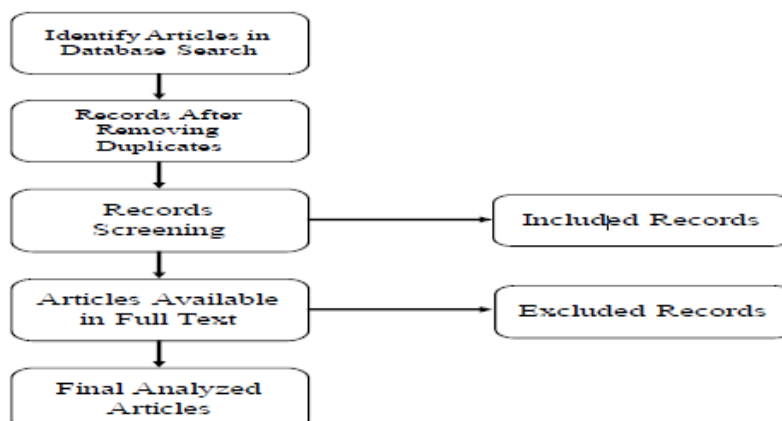
• Review Questions

Review Questions No.	Review question	Motivation
RQ1	What are the most common research designs applied?	This question investigates the predominant research designs employed in the development of maturity models.
RQ2	What are the most common research methods applied?	This question investigates the predominant research methods employed in the development of maturity models.
RQ3	What are the most common theoretical foundations to develop maturity models?	This question investigates the key theoretical underpinnings that guide the development of maturity models.
RQ4	How are the developed maturity models validated?	This question investigates the methods used to validate that maturity models are suitable for their intended purpose.
RQ5	In what domains is maturity model research applied?	This question investigates the breadth of application for the concept of maturity models across diverse domains.

• Scope of the Study

The principal objective of this investigation is to assess the prevalent maturity models within the field of information systems research. The scope of this study concentrates on articles published in leading academic outlets on information systems, encompassing both journal publications and conference proceedings. Accordingly, a concept-driven approach was selected, as this is the most widely adopted methodology in systematic reviews for developing and evaluating literature. Grounded in the concept-centric approach, the study devised a systematic classification process to identify the relevant literature.

• Search Process



• Selection of Data Sources and Search Strategy

The primary objective of the study selection process was to identify the primary studies that provide direct evidence regarding the research question (Kitchenham, B. and Charters, S., 2007). The conducted mapping study and the selection of data sources were based on electronic databases. The term "Maturity Model" was utilized in this search, but combinations of keywords were also explored to test for synonyms employed in the literature and to cover a variety of maturity model publications. The search strategy for all terms was to locate the individual words, for instance, in the title, abstract, or keywords of the articles. The search terms utilized were as follows:

- Model of maturity
- Capability model
- Assessment model
- improvement model

The search terms were combined using the Boolean "OR" operator, meaning that any sources containing any of the search terms would be retrieved.

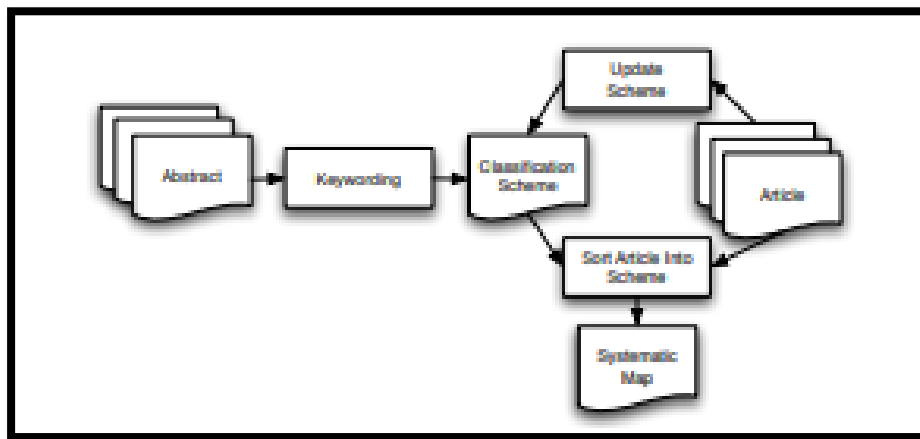
• Inclusion and Exclusion Criteria

Inclusion Criteria	Exclusion Criteria
• Directly related to the maturity model.	• Irrelevant to the study of maturity model.
• Maturity model development in the information system.	• Not peer-reviewed papers.
• Peer-reviewed.	• White paper.
• Written in English.	• Duplicate publication.
	• Journals not accessible online.
	• Not written in English.

• Classification Scheme

Developing a classification scheme is crucial for identifying existing maturity models. For this study, a concept-centric approach was selected, as it is the predominant method used in systematic reviews for developing and evaluating literature. Guided by this concept-centric approach, the study devised a systematic classification process to locate relevant studies in the literature. Consequently, a classification scheme was established based on systematic mapping studies in software engineering, as shown in the below Figure, to organise and analyse the identified articles.

Building the Classification Scheme. Source: (Petersen, K. et al., 2008)



The study utilized a concept-driven approach to develop the final classification scheme in pursuit of its objectives. The conceptual categories employed for this purpose were:

- Maturity Model Research design (9 Articles identified).
- Maturity Model Research method (9 Articles identified).
- Maturity Model Research theoretical foundations (6 Articles identified).
- Maturity Model Research Validation Approach (10 Articles identified).
- Maturity Model Research Applied Domains (13 Articles identified).

The five review questions and their corresponding research findings are presented below.

Q1: What are the most common research designs applied to develop maturity models?

The development of maturity models involves several research designs that help ensure both theoretical robustness and practical applicability. Common research designs include empirical research, design-oriented approaches, conceptual research, and several participatory and qualitative methods. Below are some of the most widely used research designs for developing maturity models.

1. Empirical Research Design

Empirical research design is a widely used approach for developing maturity models. This design involves the collection and analysis of real-world data to validate and refine the maturity model. Röglinger et al. (2012) suggest that empirical studies, often conducted through surveys, case studies, and interviews, are vital for assessing the practical applicability of maturity models. By applying empirical methods, researchers can ensure that the model reflects actual organisational practices and capabilities.

2. Design-Oriented Approach

A design-oriented approach focuses on creating artifacts, such as models or frameworks, to address specific problems in a structured way. This approach often draws from Design Science Research (DSR), a methodology that emphasizes the creation, evaluation, and iterative refinement of maturity models (Gregor & Hevner, 2013). DSR is a particularly common research design in the development of maturity models, as it combines theoretical development

with practical problem-solving. DSR involves cycles of building, evaluating, and refining models to ensure they are both theoretically sound and applicable in real-world settings.

3. Conceptual Research Design

A conceptual research design focuses on the theoretical development of a maturity model, often synthesizing insights from existing literature. Becker et al. (2009) argue that conceptual designs are essential for ensuring that maturity models are grounded in established theories, such as systems theory or organisational learning. Conceptual designs typically precede empirical testing and are used to construct the model's framework before it is subjected to real-world validation.

This design often involves literature reviews, theoretical synthesis, and conceptual mapping to build a maturity model that can be validated through subsequent empirical or design-oriented approaches.

4. Design Science Research

Design Science Research (DSR) is a key research design in the development of maturity models. DSR focuses on creating and evaluating artifacts, such as maturity models, through iterative cycles of development, evaluation, and refinement. According to Peffers et al. (2007), DSR is particularly well-suited for maturity model research because it allows for the continuous improvement of the model based on practical applications and feedback. The design and evaluation phases are repeated until the maturity model reaches a level of theoretical and practical reliability.

5. Case Study Research

Case study research is another widely applied research design in maturity model development. According to Yin (2018), case studies provide an in-depth understanding of how maturity models work in real-world environments. Researchers often apply the maturity model to specific organisational contexts and then use qualitative and quantitative data to refine the model. Case study research offers valuable insights into the practical applicability of the maturity model and is frequently used for both the development and validation phases.

6. Action Research

Action research is a participatory method where researchers work collaboratively with organisations to implement and refine the maturity model. Avison et al. (1999) argue that action research is particularly useful for maturity models because it involves continuous feedback from practitioners, allowing for real-time improvements. In action research, the maturity model is applied to organisational processes, and the outcomes are used to iteratively refine and improve the model. This method is especially effective in dynamic environments where ongoing adjustments to the model are necessary.

7. Grounded Theory

Grounded theory is a qualitative research design that allows researchers to build theory based on empirical data, typically collected through interviews, observations, and content analysis. In the context of maturity model development, grounded theory helps identify patterns and themes from real-world practices that can be incorporated into the model (Glaser & Strauss, 1967). Urquhart et al. (2010) emphasize that grounded theory is particularly useful for identifying the key dimensions and factors that should be included in the model, ensuring that it reflects actual organisational experiences.

8. Mixed Methods

Many researchers combine qualitative and quantitative research designs in the form of mixed methods. This approach allows researchers to benefit from the depth of qualitative insights (e.g., from case studies, interviews, or grounded theory) and the breadth of quantitative validation (e.g., surveys or statistical analysis). According to Venkatesh et al. (2013), mixed methods provide a more comprehensive understanding of the maturity model's effectiveness by integrating both theoretical and empirical evidence.

Conclusion

The development of maturity models relies on a variety of research designs, including empirical research, design-oriented approaches, conceptual research, Design Science Research, case studies, action research, and grounded theory. These designs allow researchers to create robust models that are both theoretically sound and practically relevant. Mixed methods are particularly useful, as they combine the strengths of qualitative and quantitative approaches, ensuring that maturity models are validated from multiple perspectives.

Identified Articles as per the Classification Scheme (9 Articles)

No.	Article Reference
1	Avison, D., Lau, F., Myers, M. & Nielsen, P.A., 1999. Action research. <i>Communications of the ACM</i> , 42(1), pp.94-97.
2	Becker, J., Knackstedt, R. & Pöppelbuß, J., 2009. Developing Maturity Models for IT Management. <i>Business & Information Systems Engineering</i> , 1(3), pp.213-222.
3	Glaser, B.G. & Strauss, A.L., 1967. <i>The Discovery of Grounded Theory: Strategies for Qualitative Research</i> . New York: Aldine.
4	Gregor, S. & Hevner, A.R., 2013. Positioning and presenting design science research for maximum impact. <i>MIS Quarterly</i> , 37(2), pp.337-355.
5	Peffer, K., Tuunanen, T., Rothenberger, M.A. & Chatterjee, S., 2007. A design science research methodology for information systems research. <i>Journal of Management Information Systems</i> , 24(3), pp.45-77.
6	Röglinger, M., Pöppelbuß, J. & Becker, J., 2012. Maturity models in business process management. <i>Business Process Management Journal</i> , 18(2), pp.328-346.
7	Urquhart, C., Lehmann, H. & Myers, M.D., 2010. Putting the “theory” back into grounded theory: Guidelines for grounded theory studies in information systems. <i>Information Systems Journal</i> , 20(4), pp.357-381.
8	Venkatesh, V., Brown, S.A. & Bala, H., 2013. Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. <i>MIS Quarterly</i> , 37(1), pp.21-54.
9	Yin, R.K., 2018. <i>Case Study Research and Applications: Design and Methods</i> . 6th ed. Los Angeles: Sage.

Q2: What are the most common research methods applied to develop maturity models?

The development of maturity models typically involves a range of research methods that help build, refine, and validate these models. These methods can be qualitative, quantitative, or a combination of both (mixed methods), and are chosen based on the specific requirements of the research context. Below are some of the most commonly applied research methods in the development of maturity models.

1. Concept Development

Concept development is one of the initial steps in building a maturity model. This involves synthesizing existing literature, frameworks, and theoretical concepts to define the core elements of the model. **Becker et al. (2009)** argue that the conceptual development of maturity models often relies on an analysis of existing models and adapting them to new contexts or domains. The result is a conceptual framework that forms the basis for subsequent empirical validation.

2. Workshops

Workshops are a common method used in the collaborative development and refinement of maturity models. In this method, practitioners, experts, and stakeholders are brought together to discuss and co-create the structure and stages of the model. According to **De Bruin et al. (2005)**, workshops provide valuable feedback from stakeholders and can help refine the conceptual foundation of the model while ensuring its relevance and practicality for the intended audience.

3. Focus Groups

Focus groups are another qualitative method frequently used in maturity model development. Similar to workshops, focus groups involve gathering a small group of stakeholders or experts to discuss and evaluate the various components of a maturity model. Focus groups help gather diverse perspectives and ensure that the model aligns with real-world experiences and needs. **Krueger and Casey (2014)** emphasize that focus groups are particularly useful for obtaining in-depth qualitative feedback during the early stages of model development.

4. Action Research

Action research is a participatory method used in the development of maturity models, where researchers collaborate with practitioners to apply and refine the model in real-world settings (Susman & Evered, 1978). This method allows for continuous feedback and iteration, making it highly effective for developing maturity models that are both practical and theoretically sound. According to **Avison et al. (1999)**, action research is particularly valuable in dynamic and complex environments, as it allows for real-time testing and adaptation of the model based on organisational feedback.

5. Delphi Method

The **Delphi method** is a structured communication technique used to gather consensus from a panel of experts, which is particularly useful for defining the levels and dimensions of a maturity model. This method involves multiple rounds of surveys or questionnaires, with feedback being provided after each round until a consensus is reached (Okoli & Pawlowski, 2004). In maturity model development, the Delphi method is often used to validate the structure and content of the model by involving a diverse set of experts in the domain.

6. Qualitative Methods

Qualitative research methods, such as **interviews** and **content analysis**, are commonly used in the early stages of maturity model development. These methods help gather insights from stakeholders, practitioners, and experts regarding their experiences, challenges, and needs (Pöppelbuß & Röglinger, 2011). Interviews, in particular, provide in-depth data on how organisations perceive their maturity in specific areas, such as data governance or information systems.

7. Quantitative Methods

Quantitative methods, such as **surveys**, are often employed in later stages of maturity model development to validate the model's structure and assess its applicability across a wider sample (Röglinger et al., 2012). **Factor analysis** and **structural equation modelling** are commonly used to analyse the relationships between the various dimensions and levels of the model, ensuring its reliability and validity. These methods provide statistical rigor and allow researchers to generalize their findings to a broader population.

8. Mixed Methods

Mixed methods research combines both qualitative and quantitative techniques to develop and validate maturity models. This approach allows researchers to benefit from the depth of qualitative data and the breadth of quantitative analysis. According to **Venkatesh et al. (2013)**, mixed methods research is particularly useful for maturity model development, as it enables a comprehensive understanding of both the theoretical foundations and the practical applications of the model. For instance, a maturity model may be initially developed through qualitative

interviews and workshops, followed by quantitative surveys to validate its structure across a larger population.

Conclusion

The development of maturity models requires a combination of research methods that are both qualitative and quantitative. Common methods include concept development, workshops, focus groups, action research, the Delphi method, and qualitative and quantitative methods. Mixed methods are particularly effective in combining the strengths of both qualitative insights and quantitative validation, ensuring that the maturity model is both theoretically sound and practically applicable.

Identified Articles as per the Classification Scheme (9 Articles)

No.	Article Reference
1	Avison, D., Lau, F., Myers, M. & Nielsen, P.A., 1999. Action research. <i>Communications of the ACM</i> , 42(1), pp.94-97.
2	Becker, J., Knackstedt, R. & Pöppelbuß, J., 2009. Developing Maturity Models for IT Management. <i>Business & Information Systems Engineering</i> , 1(3), pp.213-222.
3	De Bruin, T., Rosemann, M., Freeze, R. & Kulkarni, U., 2005. Understanding the main phases of developing a maturity assessment model. In: <i>Proceedings of the 16th Australasian Conference on Information Systems (ACIS)</i> . Sydney: ACIS, pp.1-10.
4	Krueger, R.A. & Casey, M.A., 2014. <i>Focus Groups: A Practical Guide for Applied Research</i> . 5th ed. Los Angeles: Sage.
5	Okoli, C. & Pawlowski, S.D., 2004. The Delphi method as a research tool: an example, design considerations and applications. <i>Information & Management</i> , 42(1), pp.15-29.
6	Pöppelbuß, J. & Röglinger, M., 2011. What makes a useful maturity model? A framework of general design principles for maturity models and its demonstration in business process management. In: <i>ECIS 2011 Proceedings</i> . Helsinki: AIS, pp.1-13.
7	Röglinger, M., Pöppelbuß, J. & Becker, J., 2012. Maturity models in business process management. <i>Business Process Management Journal</i> , 18(2), pp.328-346.
8	Susman, G.I. & Evered, R.D., 1978. An assessment of the scientific merits of action research. <i>Administrative Science Quarterly</i> , 23(4), pp.582-603.
9	Venkatesh, V., Brown, S.A. & Bala, H., 2013. Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. <i>MIS Quarterly</i> , 37(1), pp.21-54.

Q3: What are the most common theoretical foundations for developing maturity models?

The development of maturity models is typically based on well-established theoretical foundations that provide a structured and meaningful framework for assessing the progression of an organisation's capabilities. The most common theoretical foundations used in the development of maturity models are capability maturity model theory, concept construction, systems theory, organisational learning, and the resource-based view (RBV). These theories provide a foundation for understanding the stages of development that organisations undergo as they strive for continuous improvement and higher levels of performance.

1. Capability Maturity Model Theory

Capability Maturity Model (CMM) theory forms the core of many maturity models, particularly those designed for software development, information systems, and process improvement. This theory was first introduced by the Software Engineering Institute (SEI) and is structured around five levels of maturity: Initial, Managed, Defined, Quantitatively Managed, and Optimizing (Paulk et al., 1993). The CMM framework provides a structured approach for measuring and improving organisational capabilities, and it has been adapted for various domains, including data governance and business process management.

CMM theory emphasizes the gradual improvement of capabilities, with each level representing a more advanced state of organisational performance. According to **Paulk et al. (1993)**, the maturity model theory helps organisations identify weaknesses, set priorities, and implement changes to move toward higher levels of capability.

2. Concept Construction

Concept construction refers to the process of developing a theoretical model or framework based on a comprehensive analysis of existing literature and theory. In the context of maturity models, concept construction often involves the adaptation of existing theories or models to new domains. **Becker et al. (2009)** argue that the construction of maturity models relies on synthesizing and integrating previous models, theoretical concepts, and empirical findings to create a coherent structure that reflects the stages of organisational maturity.

This theoretical foundation is particularly important in ensuring that the maturity model is grounded in established concepts, which helps enhance its credibility and applicability in various domains. By constructing concepts from existing theory, researchers can ensure that the maturity model is both theoretically sound and relevant to current organisational practices.

3. Systems Theory

Systems theory, developed by **Ludwig von Bertalanffy (1968)**, emphasizes the interconnectedness of different components within an organisation and how these components must work together to achieve higher levels of maturity. Systems theory views an organisation as a complex system made up of interrelated parts that must function cohesively to optimize performance. In the context of maturity models, systems theory helps explain how different organisational processes, structures, and capabilities interact and evolve as the organisation matures.

Systems theory is commonly applied in maturity model development to ensure that the model reflects the interdependencies between different organisational elements, such as technology, processes, and people. By incorporating systems thinking, maturity models can provide a more holistic view of organisational growth and development.

4. Organisational Learning

Organisational learning theory, as proposed by **Argyris and Schön (1978)**, underpins many maturity models, particularly those focused on knowledge management and continuous improvement. This theory posits that organisations learn and adapt over time by systematically reflecting on their processes, experiences, and outcomes. Organisational learning models emphasize the importance of feedback loops, where organisations assess their current capabilities and identify areas for improvement.

In maturity model development, organisational learning theory is often used to justify the progression of maturity levels, as organisations learn from their experiences and gradually move toward higher levels of capability. **Becker et al. (2009)** note that maturity models grounded in organisational learning theory help organisations institutionalize best practices and create a culture of continuous improvement.

5. Resource-Based View (RBV)

The **resource-based view (RBV)** of the firm, introduced by **Wernerfelt (1984)**, focuses on the strategic resources and capabilities that give an organisation a competitive advantage.

According to RBV, organisations can achieve sustained competitive advantage by developing and leveraging unique resources, such as knowledge, skills, and technology. Maturity models based on RBV focus on the development of these critical resources and how they evolve over time to create higher levels of organisational performance.

In the context of maturity models, RBV is used to identify the key resources and capabilities that must be developed as an organisation matures. **Röglinger et al. (2012)** suggest that maturity models grounded in RBV help organisations understand which resources are most valuable at different stages of maturity and how they can be leveraged to achieve strategic goals.

Conclusion

The development of maturity models is grounded in several key theoretical foundations, each of which provides a unique perspective on how organisations progress and improve their capabilities. **Capability maturity model theory** offers a structured approach for measuring and improving performance, while **concept construction** ensures that models are grounded in established theory. **Systems theory** provides a holistic view of organisational processes, and **organisational learning** emphasizes the importance of continuous improvement. Finally, the **resource-based view** focuses on the strategic development of resources that provide competitive advantages. These theoretical foundations collectively contribute to the robustness and applicability of maturity models across different domains.

Identified Articles as per the Classification Scheme (6 Articles)

No.	Article Reference
1	Argyris, C. & Schön, D.A., 1978. <i>Organisational Learning: A Theory of Action Perspective</i> . Reading, MA: Addison-Wesley.
2	Becker, J., Knackstedt, R. & Pöppelbuß, J., 2009. Developing Maturity Models for IT Management. <i>Business & Information Systems Engineering</i> , 1(3), pp.213-222.
3	Bertalanffy, L. von, 1968. <i>General System Theory: Foundations, Development, Applications</i> . New York: George Braziller.
4	Paulk, M.C., Curtis, B., Chrissis, M.B. & Weber, C.V., 1993. Capability Maturity Model, Version 1.1. <i>IEEE Software</i> , 10(4), pp.18-27.
5	Röglinger, M., Pöppelbuß, J. & Becker, J., 2012. Maturity models in business process management. <i>Business Process Management Journal</i> , 18(2), pp.328-346.
6	Wernerfelt, B., 1984. A resource-based view of the firm. <i>Strategic Management Journal</i> , 5(2), pp.171-180.

Q4: How are the developed maturity models validated to fit their purpose in research papers?

The validation of maturity models in research papers involves the use of multiple methods to ensure their reliability, relevance, and practical applicability. Along with statistical techniques, researchers also employ various qualitative and participatory approaches, such as questionnaires, focus groups, and workshops. Below are some of the most common methods for validating maturity models, focusing on a combination of quantitative, qualitative, and mixed approaches.

1. Expert Validation

Expert validation remains one of the most popular techniques in the early stages of validating maturity models. Domain experts are engaged to assess the model's relevance, structure, and

comprehensiveness. According to Pöppelbuß and Röglinger (2011), expert panels or the Delphi method are commonly used to gather multiple rounds of feedback, helping to ensure that the maturity model is fit for purpose and aligns with industry needs. Expert input is critical for identifying any gaps in the model before it is deployed for broader empirical testing.

2. Questionnaires

Questionnaires are a widely used tool for validating maturity models, especially in the later stages of model development. Questionnaires can be distributed to a broad audience, allowing researchers to collect data from a larger sample of respondents. This method provides quantitative data that can be used to statistically test the structure and reliability of the model. Factor analysis and Cronbach's alpha are frequently employed to validate the internal consistency of the model based on responses (Hair et al., 2010). Questionnaires are particularly useful for assessing whether the dimensions of the maturity model align with real-world organisational practices (Röglinger et al., 2012).

3. Focus Groups

Focus groups provide qualitative feedback during the validation process and are often used alongside other methods such as surveys or interviews. Focus groups involve gathering a small group of experts or practitioners to discuss and provide feedback on the maturity model. Krueger and Casey (2014) argue that focus groups are effective for eliciting in-depth insights from participants, which can be used to refine and enhance the model. The discussions in focus groups allow researchers to capture qualitative nuances, making this method particularly valuable for validating the contextual relevance of the model.

4. Workshops

Workshops are collaborative forums where practitioners, stakeholders, and researchers come together to assess the validity of a maturity model. Workshops often involve practical exercises where participants apply the maturity model to real-world scenarios, providing direct feedback on its applicability and ease of use. According to De Bruin et al. (2005), workshops are particularly useful for engaging stakeholders in the validation process, as they provide an opportunity to iteratively refine the model based on hands-on experience. This participatory approach ensures that the maturity model reflects the needs of its intended users.

5. Case Studies

Case study research remains one of the most common empirical validation techniques for maturity models. Case studies allow researchers to apply the model in real-world settings and gather detailed insights on its effectiveness and accuracy. According to Yin (2018), case studies provide a robust method for assessing the maturity model's applicability across different organisational contexts, offering an opportunity to refine the model based on observed outcomes. Case studies are also beneficial for providing rich, contextual data that can highlight any limitations of the model.

6. Survey-Based Validation

Surveys are a quantitative method frequently employed to gather data from a large sample of organisations, helping researchers validate the maturity model's structure and relevance. Surveys can capture responses from a diverse set of organisations, allowing researchers to test the generalizability of the model across different industries or domains. The results from surveys are often analysed using statistical techniques such as regression analysis, factor analysis, and structural equation modelling (SEM) (Hair et al., 2010). These techniques provide statistical validation of the model's dimensions and help establish its reliability.

7. Statistical Validation Techniques

Statistical techniques are essential for ensuring the robustness of maturity models. Some of the most commonly used techniques include:

- Factor Analysis: Used to identify the underlying structure of the model by grouping related variables, this method ensures that the model's dimensions are coherent and well-defined (Hair et al., 2010).
- Cronbach's Alpha: This technique measures the internal consistency of the model's constructs, ensuring that the dimensions and indicators reliably measure the intended concepts. A Cronbach's alpha value of 0.7 or above is considered acceptable for validation (Hair et al., 2010).
- Structural Equation Modelling (SEM): SEM helps researchers validate the relationships between latent variables in the maturity model, providing a comprehensive statistical assessment of its structure (Kline, 2015).
- Regression Analysis: Regression analysis is used to test whether the model's stages of maturity are predictive of certain outcomes, such as organisational performance, and can confirm the model's external validity (Röglinger et al., 2012).

8. Action Research

Action research is a participatory method in which researchers collaborate with practitioners to validate and refine the maturity model in real-world settings. According to Avison et al. (1999), action research allows for continuous feedback and iteration, making it particularly effective for validating models in dynamic environments. This method focuses on problem-solving within organisations and provides practical insights that can be used to further develop the model.

9. Mixed Methods Validation

A mixed methods approach combines qualitative and quantitative techniques to ensure comprehensive validation of the maturity model. This method allows researchers to leverage the depth of qualitative data, such as interviews and focus groups, alongside the breadth of quantitative data gathered from surveys (Venkatesh et al., 2013). Mixed methods validation provides a holistic view of the model's effectiveness and ensures that it is both theoretically robust and practically relevant.

Conclusion

The validation of maturity models involves a combination of qualitative and quantitative methods, including expert validation, questionnaires, focus groups, workshops, case studies, and survey-based validation. Statistical techniques such as factor analysis, Cronbach's alpha, structural equation modelling, and regression analysis are frequently employed to provide rigorous validation of the model's structure. The use of mixed methods, along with participatory approaches like workshops and action research, ensures that the model is both relevant to its intended users and grounded in empirical evidence.

Identified Articles as per the Classification Scheme (10 Articles)

No.	Article Reference
1	Avison, D., Lau, F., Myers, M. & Nielsen, P.A., 1999. Action research. <i>Communications of the ACM</i> , 42(1), pp.94-97.
2	Becker, J., Knackstedt, R. & Pöppelbuß, J., 2009. Developing Maturity Models for IT Management. <i>Business & Information Systems Engineering</i> , 1(3), pp.213-222.
3	De Bruin, T., Rosemann, M., Freeze, R. & Kulkarni, U., 2005. Understanding the main phases of developing a maturity assessment model. In: <i>Proceedings of the 16th Australasian Conference on Information Systems (ACIS)</i> . Sydney: ACIS, pp.1-10.
4	Hair, J.F., Black, W.C., Babin, B.J. & Anderson, R.E., 2010. <i>Multivariate Data Analysis</i> . 7th ed. Upper Saddle River, NJ: Prentice Hall.

No.	Article Reference
5	Kline, R.B., 2015. <i>Principles and Practice of Structural Equation Modelling</i> . 4th ed. New York: Guilford Press.
6	Krueger, R.A. & Casey, M.A., 2014. <i>Focus Groups: A Practical Guide for Applied Research</i> . 5th ed. Los Angeles: Sage.
7	Pöppelbuß, J. & Röglinger, M., 2011. What makes a useful maturity model? A framework of general design principles for maturity models and its demonstration in business process management. In: <i>ECIS 2011 Proceedings</i> . Helsinki: AIS, pp.1-13.
8	Röglinger, M., Pöppelbuß, J. & Becker, J., 2012. Maturity models in business process management. <i>Business Process Management Journal</i> , 18(2), pp.328-346.
9	Venkatesh, V., Brown, S.A. & Bala, H., 2013. Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. <i>MIS Quarterly</i> , 37(1), pp.21-54.
10	Yin, R.K., 2018. <i>Case Study Research and Applications: Design and Methods</i> . 6th ed. Los Angeles: Sage.

Q5: In what domains is maturity model research applied?

Maturity model research has been applied across a wide range of domains, demonstrating its versatility and adaptability in assessing and improving processes, systems, and organisational capabilities. The concept of maturity models, originally developed in the context of software development, has since been expanded to numerous other fields, reflecting its utility in both technical and managerial disciplines. Below is an overview of some key domains where maturity models are applied.

1. E-Government

Maturity models have been extensively used in the domain of e-government to assess the progression of governmental institutions in adopting digital solutions. E-government maturity models evaluate the development of online services, citizen engagement, and inter-organisational collaboration within public sector entities. According to Layne and Lee (2001), e-government maturity models are often structured around stages that reflect the evolution from simple online presence to fully integrated digital services.

2. Software Development and Software Engineering

The Capability Maturity Model Integration (CMMI) is the most well-known maturity model in software development and software engineering. Originally developed by the Software Engineering Institute (SEI), CMMI is widely applied to improve software development processes by assessing organisations' capabilities across five levels of maturity (Paulk et al., 1993). This model has become a standard in software engineering and has been adapted for various other domains.

3. Project Management

Maturity models are widely applied in project management to help organisations improve their project delivery capabilities. According to Cooke-Davies (2004), project management maturity models provide a structured framework for assessing and improving processes related to planning, execution, and control of projects. Models such as the Project Management Maturity Model (PMMM) offer stages that guide organisations toward higher levels of project management efficiency.

4. Mobile Learning

The use of maturity models in mobile learning has gained traction as educational institutions adopt mobile technologies to enhance learning. Maturity models in this domain assess how institutions evolve from initial, ad-hoc implementations of mobile learning to fully integrated, pedagogically sound systems. Kurt (2017) notes that maturity models in mobile learning help guide institutions through the various stages of technology adoption and curriculum integration.

5. Cloud Computing

Maturity models for cloud computing are applied to assess how organisations adopt and utilize cloud technologies. These models evaluate readiness, strategy, deployment, and optimization of cloud services, helping organisations achieve scalable and secure cloud environments. **Linthicum (2010)** suggests that cloud computing maturity models guide organisations through the stages of cloud adoption, ensuring that they effectively manage cloud resources and governance.

6. Governance, Risk Management, and Compliance (GRC)

In the domain of governance, risk management, and compliance (GRC), maturity models are used to evaluate how well organisations manage regulatory requirements and risk mitigation processes. Sadiq et al. (2007) argue that GRC maturity models help organisations develop stronger compliance frameworks by assessing their policies, procedures, and overall risk management capabilities.

7. Information Security

Maturity models are widely used in information security to assess the progression of security practices and protocols within organisations. Mettler and Rohner (2009) suggest that information security maturity models, such as those based on the ISO/IEC 27001 framework, help organisations develop robust security postures, ensuring that they have the necessary processes in place to protect data and systems.

8. IT Governance

Maturity models are applied in IT governance to assess how well organisations manage and align their IT resources with business objectives. The COBIT maturity model, developed by ISACA, is a widely used framework for assessing IT governance capabilities. Weill and Ross (2004) note that IT governance maturity models provide organisations with a structured approach for improving IT decision-making processes and aligning IT investments with business goals.

9. Interoperability and Collaboration

Maturity models in interoperability and collaboration are used to assess how well organisations work together, both within and across industry sectors. Chen et al. (2008) emphasize that maturity models in this domain help organisations evaluate their capability to share information, resources, and services with external partners, ensuring effective and efficient collaboration.

10. Business Intelligence

Maturity models are applied in business intelligence (BI) to assess how organisations use data and analytics to support decision-making. BI maturity models evaluate how organisations move from basic reporting capabilities to advanced predictive and prescriptive analytics. Watson (2009) highlights that BI maturity models help organisations develop their data capabilities, enabling them to make more informed decisions and gain a competitive advantage.

11. Telemedicine

In telemedicine, maturity models are used to assess the development and integration of remote healthcare technologies. These models evaluate how healthcare providers evolve from initial telemedicine implementations to fully integrated, patient-centric systems. Yellowlees (2005)

notes that telemedicine maturity models guide healthcare organisations through the stages of adopting telehealth technologies, ensuring both clinical and operational success.

12. Information Systems

Maturity models have their roots in information systems (IS), where they are used to assess the progression of IS capabilities within organisations. Nolan's Stages Theory, one of the earliest IS maturity models, outlines the evolution of information systems from ad-hoc use to fully integrated systems that support strategic decision-making (Nolan, 1979). IS maturity models continue to be widely used for evaluating the development and management of IT resources.

13. Data Governance

In the domain of data governance, maturity models are used to assess an organisation's ability to manage data as a strategic asset. Ladley (2019) argues that data governance maturity models help organisations evaluate their processes for data stewardship, quality management, and compliance, ensuring that they can effectively control and secure their data assets.

14. Supply Chain Management

Maturity models are frequently applied in supply chain management (SCM) to assess the development of supply chain processes, from basic operations to fully optimized and integrated systems. Lockamy and McCormack (2004) note that SCM maturity models provide a structured approach for improving efficiency, collaboration, and risk management across supply chains.

15. Cybersecurity

In cybersecurity, maturity models assess the development of an organisation's security practices and defence mechanisms. Cline et al. (2019) suggest that cybersecurity maturity models, such as the NIST Cybersecurity Framework, help organisations develop capabilities to identify, protect, detect, respond, and recover from cyber threats.

16. Knowledge Management

Knowledge management (KM) maturity models are used to assess how well organisations capture, store, and leverage knowledge assets. According to Gold et al. (2001), KM maturity models help organisations progress from ad-hoc knowledge sharing to fully integrated knowledge management systems that enhance innovation and organisational learning.

Conclusion

Maturity models have been applied across a wide range of domains, from e-government and software development to cybersecurity and knowledge management, reflecting their versatility and adaptability. The concept of maturity models is applicable to both technical and managerial disciplines, offering organisations a structured way to assess and improve their processes, capabilities, and systems.

Identified Articles as per the Classification Scheme (13 Articles)

No.	Article Reference
1	Chen, D., Doumeingts, G. & Vernadat, F., 2008. Architectures for enterprise integration and interoperability: Past, present and future. <i>Computers in Industry</i> , 59(7), pp.647-659.
2	Cline, R., Haynes, J. & King, J., 2019. <i>NIST Cybersecurity Framework: A Guide for Leaders</i> . National Institute of Standards and Technology.
3	Cooke-Davies, T., 2004. Project management maturity models. <i>The Project Management Journal</i> , 35(1), pp.32-43.
4	Gold, A.H., Malhotra, A. & Segars, A.H., 2001. Knowledge management: An organisational capabilities perspective. <i>Journal of Management Information Systems</i> , 18(1), pp.185-214.

No.	Article Reference
5	Kurt, S., 2017. A literature review on mobile learning. <i>Educational Technology Research and Development</i> , 65(1), pp.1-19.
6	Ladley, J., 2019. <i>Data Governance: How to Design, Deploy, and Sustain an Effective Data Governance Program</i> . 2nd ed. San Diego: Academic Press.
7	Layne, K. & Lee, J., 2001. Developing fully functional e-government: A four stage model. <i>Government Information Quarterly</i> , 18(2), pp.122-136.
8	Linthicum, D.S., 2010. <i>Cloud Computing and SOA Convergence in Your Enterprise: A Step-by-Step Guide</i> . Boston: Addison-Wesley.
9	Lockamy, A. & McCormack, K., 2004. The development of a supply chain management process maturity model using the concepts of business process orientation. <i>Supply Chain Management: An International Journal</i> , 9(4), pp.272-278.
10	Mettler, T. & Rohner, P., 2009. Situational maturity models as instrumental artifacts for organisational design. In: <i>Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology</i> . Philadelphia: ACM.
11	Nolan, R.L., 1979. Managing the crisis in data processing. <i>Harvard Business Review</i> , 57(2), pp.115-126.
12	Sadiq, S., Governatori, G. & Namiri, K., 2007. Modelling control objectives for business process compliance. In: <i>International Conference on Business Process Management</i> . Brisbane: Springer.
13	Watson, H.J., 2009. Business intelligence maturity models: The state of the art. <i>Information Systems Management</i> , 26(1), pp.30-41.

Appendix N: HDG Model Validation

Respondents Background

Please specify your organisation's size of employees.

More than 5,000

1,000 - 5,000

100 - 1,000

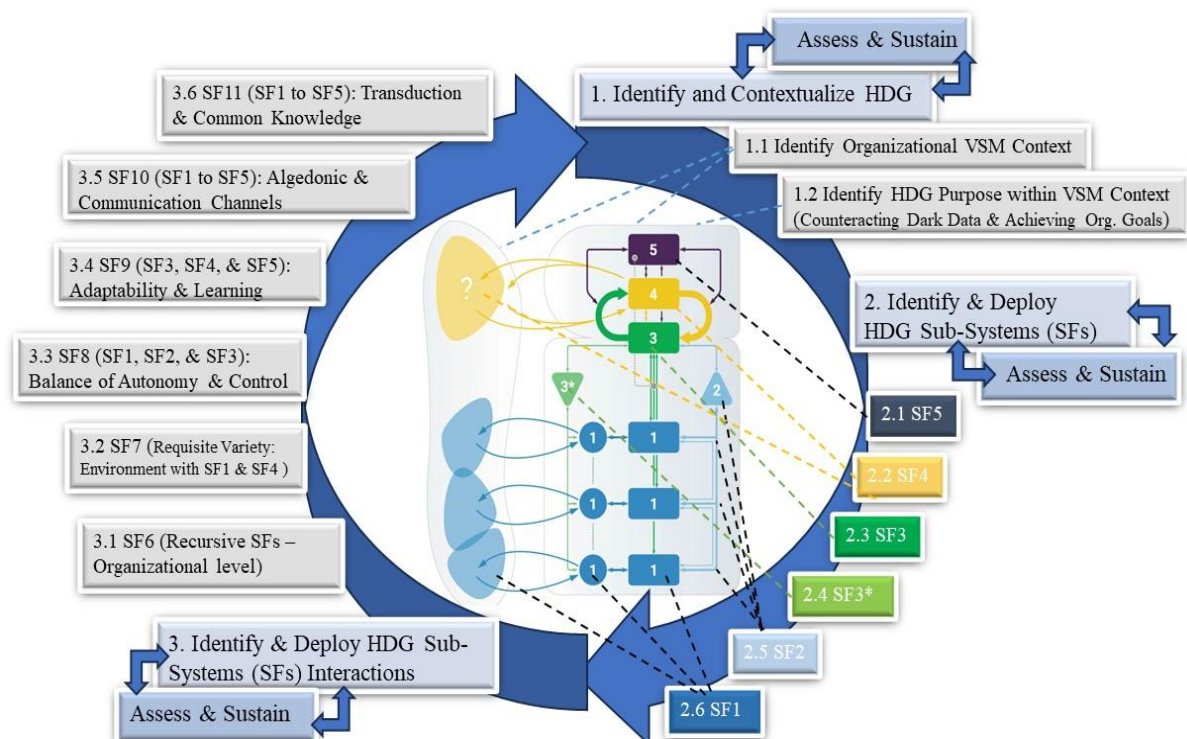
Less than 100

How many years of experience have you had in this current job?

Your experience in data governance (optional):

Your experience in governance aspects (optional):

A Strategy Framework to Design, Deploy and Sustain an Effective Dark Data Governance Model.



Questionnaire 1: Round 1 Questions:

- **Distribute the questions in Round 1 to validate the proposed model in order to:**
 - **Validate the HDG model systemic design within the VSM context to counteract dark data and support the achievement of the organisational goals.**

Please Rate the extent to which you agree or disagree with the following statements 1= Strongly disagree 2= Disagree 3= Neutral 4= Agree 5= strongly agree		
Validate the HDG model systemic design within the Organisational VSM context		
St. 1.n	Statement	Rating (1-5)
1.1	The model provides a methodology to deploy, assess, and sustain an effective holistic dark data governance model	
1.2	The model provides a structured methodology for supporting decision-makers to understand important systemic functions to deploy, assess, and sustain dark data governance subsystems within an organisational context.	
1.3	The model supports organisational continuous learning, corporate harmonization, and change management in handling dark data issues and achieving organisational goals.	
1.4	The model ensures effective and responsive operational units by balancing autonomy with control through coordinated data governance activities. This supports decision-making and the achievement of operational and organisational goals.	
1.5	The model supports adaptability and the achievement of long-term goals by effectively addressing dark data constraints and leveraging data opportunities	
1.6	The Model establishes, evaluates, and enhances corporate holistic data governance policies, ensuring a consistent operational framework to counteract dark data. It balances dark data governance internal and external perspectives to support the achievement of the current and future goals.	
1.7	The Model manages the complexity of the environment by responding to digital data disruptions and emerging data and data governance regulations. This enables the organisation to remain agile in achieving its goals and maintain stability.	
1.8	The model will help organisations to reduce the cost, time, and effort involved in counteracting dark data and achieving its goals.	
1.9	The model ensures accuracy and compliance with data governance standards, supporting corrective actions and achievement of the organisational goals.	
1.10	The model has immediate interventions to ensure organisational goal achievement and rapid response to high dark data risks.	

o Validate the HDG model's key systemic phases within the Organisational VSM Context to counteract dark data and support the achievement of the organisational goals.

Please Rate the extent to which you agree or disagree with the following statements 1= Strongly disagree 2= Disagree 3= Neutral 4= Agree 5= strongly agree		
Validate the HDG model's key systemic phases within the Organisational VSM context to counteract dark data and support the achievement of the organisational goals.		
Phase ID	HDGM Systemic Phase Description	Rating (1-5)
Phase 1	Contextualize HDGM: Identifying the organisational system-in-focus within the Viable System Model is vital to contextualize, assess, and sustain the holistic data governance model (HDGM) as a subsystem within the system-in-focus. This is crucial to identify the organisation's goals and objectives and the goals of the holistic data governance model to mitigate dark data risks and support organisational viability and goal attainment.	
Phase 2	HDGM Key Systemic Functions: Identifying, deploying, assessing, and sustaining the systemic functions of the holistic data governance model (HDGM) within the five subsystems of the Viable System Model is essential to counteract dark data and support the achievements of the organisational objectives. This is crucial to deploy, assess, and sustain the corporate policies developed for key data governance domains, as well as harmonization, cohesion, autonomy, auditing, compliance, adaptation to the environment, and the overall data governance direction to ensuring a balance between current and future functions.	
Phase 3	Key Interactions among HDGM Systemic Functions: Identifying, deploying, assessing, and sustaining the key interactions among the holistic data governance systemic functions (HDG SFs) within the five subsystems of the Viable System Model is essential to counteract dark data and support the achievements of the organisational objectives. This integrated approach with IT and corporate governance is crucial to governing data assets, addressing dark data risks arising from external disruptions, identifying dark data types, promoting organisational agility in handling dark data risks, enhancing decision-making, balancing the holistic data governance model's present and future orientations as well as internal and external perspectives, support learning and change management, and enable immediate interventions in high-risk dark data situations.	

Which additional phases to the Model do you think would be helpful in terms of supporting the deployment and sustainability of the dark data governance holistic model within the organisational VSM context?

.....

Are there any phases in the model which you think would not be helpful in terms of supporting the deployment and sustainability of the dark data governance holistic model within the organisational VSM context?

.....

Questionnaire 2: Round 2 Questions:

- Refining and validating questions and responses from Round 1 as necessary; **Distribute the questions in Round 2 to validate the proposed model in order to:**
 - o **Validate the HDG systemic functions of the model under each systemic phase within the VSM context to counteract dark data risks and support the achievement of the organisational goals.**

• Systemic Phase 1 - Contextualize HDGM

Please Rate the extent to which you agree or disagree with the following statements 1= Strongly disagree 2= Disagree 3= Neutral 4= Agree 5= strongly agree		
Validate the HDG systemic functions of the model under systemic phase 1 (Contextualize HDGM) within the VSM context to counteract dark data risks and support the achievement of the organisational goals		
SF. 1.n	Systemic Function	Rating (1-5)
SF 1.1	Identify the organisational VSM system-in-focus (Organisational level) with its purpose, goals, stakeholders, and boundaries of the organisation within its environment. Define dark data governance purpose. Dark Data governance purpose for this study is to counteract dark data risks and create business value to support organisational viability and goal achievement.	
SF 1.2	Contextualize, deploy and sustain the scope to support the goals of the holistic data governance model (HDGM) as a subsystem within the	

	organisational VSM system-in-focus. The goal is mainly to counteract dark data risks and support organisational viability and goal achievement.	

Which additional systemic functions to phase 1, do you think would be helpful in terms of supporting the deployment and sustainability of the dark data governance holistic model within the organisational VSM context?

.....
.....
.....

Is there any systemic function in phase 1, which you think would not be helpful in terms of supporting the deployment and sustainability of the dark data governance holistic model within the organisational VSM context?

.....
.....
.....

- **Systemic Phase 2 – HDGM Key Systemic Functions**

Please Rate the extent to which you agree or disagree with the following statements 1= Strongly disagree 2= Disagree 3= Neutral 4= Agree 5= strongly agree		
Validate the HDG systemic functions (HDG SFs) of the model under systemic Phase 2 (HDGM Key Systemic Functions) within the VSM context to counteract dark data risks and support the achievement of the organisational goals		
SF. 2.n	Systemic Function Description	Rating (1-5)
SF 2.1	HDG SF1 Support to Operational Units (HDG SF1 within VSM S1) - identify the primary activities that deliver the organisational products or services. Deploy, and sustain HDG policies, guidelines, and procedures, to provide core activities with necessary data and counteract dark data risks. HDG SF1 supports organisational viability and the achievement of operational goals.	
SF 2.2	HDG Harmonisation (HDG SF2 within VSM S2): Define, deploy, and sustain compliance with corporate dark data governance systemic functions (e.g. corporate policies, guidelines, standards, rules, and protocols) to prevent recurrent dark data governance conflicts and misalignment among primary units within S1. Deploy identified corrective actions and continuously improve as appropriate to support corporate	

	harmonization. HDG SF2 supports organisational viability and the achievement of operational goals.	
SF 2.3	HDG Cohesion & Autonomy (HDG SF3 within VSM S3): Define, deploy, and sustain corporate dark data governance systemic functions: HDG Corporate policies, HDG performance measurements, HDG compliance requirements, HDG resource requirements (e.g. Technology, Financials, competencies) requirements, and allocation of HDG resources to SF1. Corporate policies are developed for key data governance domains: Data Architecture, Data Quality, Metadata, Data Security, Reference & Master Data, Data Warehousing/Business Intelligence/Artificial Intelligence, Data Modelling & Design, Document & Content Management, Data Storage & Infrastructure/Operation, Data Integration & Interoperability. HDG SF3 supports the balance between self-regulation (Autonomy) for each operational unit in S1 and their synergies (Cohesion) amongst them for improved organisational performance and achievement of operational and organisational goals.	
SF 2.4	HDG Audit and Compliance (HDG SF3* within S3*): Define, conduct, and sustain data governance auditing and compliance functions to gather information about data requirements and dark data challenges from S1 units. Accordingly, results and improvements are shared through key communication channels among SF3, SF3*, and SF1. This is to support the achievement of organisational goals.	
SF 2.5	HDG Intelligence /Adaptation (HDG SF4 within S4): Conduct research, development, and corporate planning to make sense of the environmental changes such as constraints and opportunities related to data needed by the organisation and potentially encountering dark data that could threaten organisational viability. Deploy, and sustain the holistic data governance strategy and long-term orientated tasks to support and improve the adaptability and the achievement of the organisation's long-term goals.	
SF 2.6	HDG Policy, Identity, and Closure (HDG SF5 within S5): Establish, deploy, and sustain the corporate integration of HDG policies with other relevant policies to continuously ensure a consistent governance context. Establish the ultimate dark data governance decision-making role within the VSM system-in-focus; thereby providing the logical closure to it. Establish the system's overall data governance direction, policies, values, and purpose and monitor the feedback loop between current (SF3) and future (SF4) data governance systemic functions (in integration with corporate IT governance and corporate governance). This ensures the balance between internal and external perspectives and supports the achievement of present operational and long-term organisational goals.	

Which additional systemic functions to phase 2, do you think would be helpful in terms of supporting the deployment and sustainability of the dark data governance holistic model within the organisational VSM context?

.....
.....
.....

Is there any systemic function in phase 2, which you think would not be helpful in terms of supporting the deployment and sustainability of the dark data governance holistic model within the organisational VSM context?

.....

.....

.....

- **Systemic Phase 3 - Key Interactions among HDGM Systemic Functions**

Please Rate the extent to which you agree or disagree with the following statements 1= Strongly disagree 2= Disagree 3= Neutral 4= Agree 5= strongly agree		
Validate the HDG systemic functions of the model under systemic phase 3 (Key Interactions among HDGM Systemic Functions) within the VSM context to counteract dark data risks and support the achievement of the organisational goals		
SF. 3.n	Systemic Function Description	Rating (1-5)
SF 3.1	HDG Recursive Systemic Functions (SF6): Identify the level of recursions for the organisation. Recursivity ensures each embedded organisation operates as a viable system itself with appropriate autonomy to self-govern. All data governance systemic functions at different levels of recursions are integrated to counteract dark data and support the achievement of operational and organisational embedded goals.	
SF 3.2	HDG Requisite Variety Systemic Function (SF7): Identify, deploy, and sustain short-term (SF1-Environment) and long-term (SF4-Environment) data governance activities within the system's environment. This is crucial to respond to data governance present and anticipated organisational data requirements and associated dark data threats to achieve organisational goals.	
SF 3.3	HDG Inter-operational Management Systemic Functions (SF8): Identify, deploy, and sustain key communication channels and key information flows among SF1, SF2, and SF3 within the VSM S1, S2, and S3. This is crucial to balance operational autonomy with data governance control through SF1 data governance support activities within S1 Operations, SF2 data governance coordination, and SF3 data governance control systemic functions. This enhances decision-making through self-regulation, cohesion, and synergy to support achieving operational and organisational goals	

SF 3.4	HDG Adaptability, Learning, and Change Management Systemic Functions (SF9): Identify, deploy, and sustain key communication channels and key information flows among the data governance metasystem functions SF3, SF4, and SF5. This is crucial to provide the organisation with data governance decision-making capabilities, balancing present and future orientations and internal and external perspectives.	
SF 3.5	HDG Communication channels and Algedonic channel Systemic Functions (SF10): Identify, deploy, and sustain key communication channels and key information flows among SF1, SF2, SF3, SF4, and SF5. In crises, the algedonic channel triggers immediate interventions from the metasystem to ensure rapid response to high dark data risks.	
SF 3.6	HDG Common Data Governance Holistic Context (SF11): Identify, deploy, and sustain the common data governance holistic context through the integration of all systemic functions (SF1 to SF5) and their integration within SF1 to SF5 to function cohesively. This ensures the organisation operates as a unified system.	

Which additional systemic functions to phase 3, do you think would be helpful in terms of supporting the deployment and sustainability of the dark data governance holistic model within the organisational VSM context?

.....
.....
.....

Is there any systemic function in phase 3, which you think would not be helpful in terms of supporting the deployment and sustainability of the dark data governance holistic model within the organisational VSM context?

.....
.....
.....

Questionnaire 3: Round 3 Questions

- Refining and validating questions and responses from Round 2 as necessary; **Distribute the questions in Round 3 to validate the proposed model in order to:**
 - o **Obtain suggestions from the participants to improve the holistic dark data governance model (HDGM).**

Are there any changes you would suggest improving the Model?

.....
.....

o Validate the usability of implementing the HDG model within the organisational VSM context to counteract dark data and support the achievement of organisational goals.

Please Rate the extent to which you agree or disagree with the following statements 1= Strongly disagree 2= Disagree 3= Neutral 4= Agree 5= strongly agree		
Validate the usability of implementing the HDGM within the organisational VSM context to counteract dark data and support the achievement of organisational goals		
St. 3.n	Statement: HDGM has the following Qualities	Rating (1-5)
3.1	The model is easy to use.	
3.2	The model is easy to learn.	
3.3	The model is clear and flexible. It can adapt to changing organisational needs and data governance requirements with agility.	
3.4	The model is scalable, allowing the application to various levels of recursion within the organisation. It is adaptable to different sizes of organisations and data sets.	
3.5	The model can be practically used and easily integrates with existing systems and technologies within the organisation.	
3.6	The model provides comprehensive systemic functions that support innovation within the organisation's context.	
3.7	The model adds value by efficiently counteracting dark data risks and supporting the achievement of organisational goals.	

- Refining and validating questions and responses from Round 3 as necessary

Appendix O: Maturity Model & Assessment Matrix Evaluation

Round 1 Questions

Respondents Background

Please specify your organisation size of employees.....

More than 5,000

1,000 - 5,000

100 - 1,000

Less than 100

What is your job role?.....

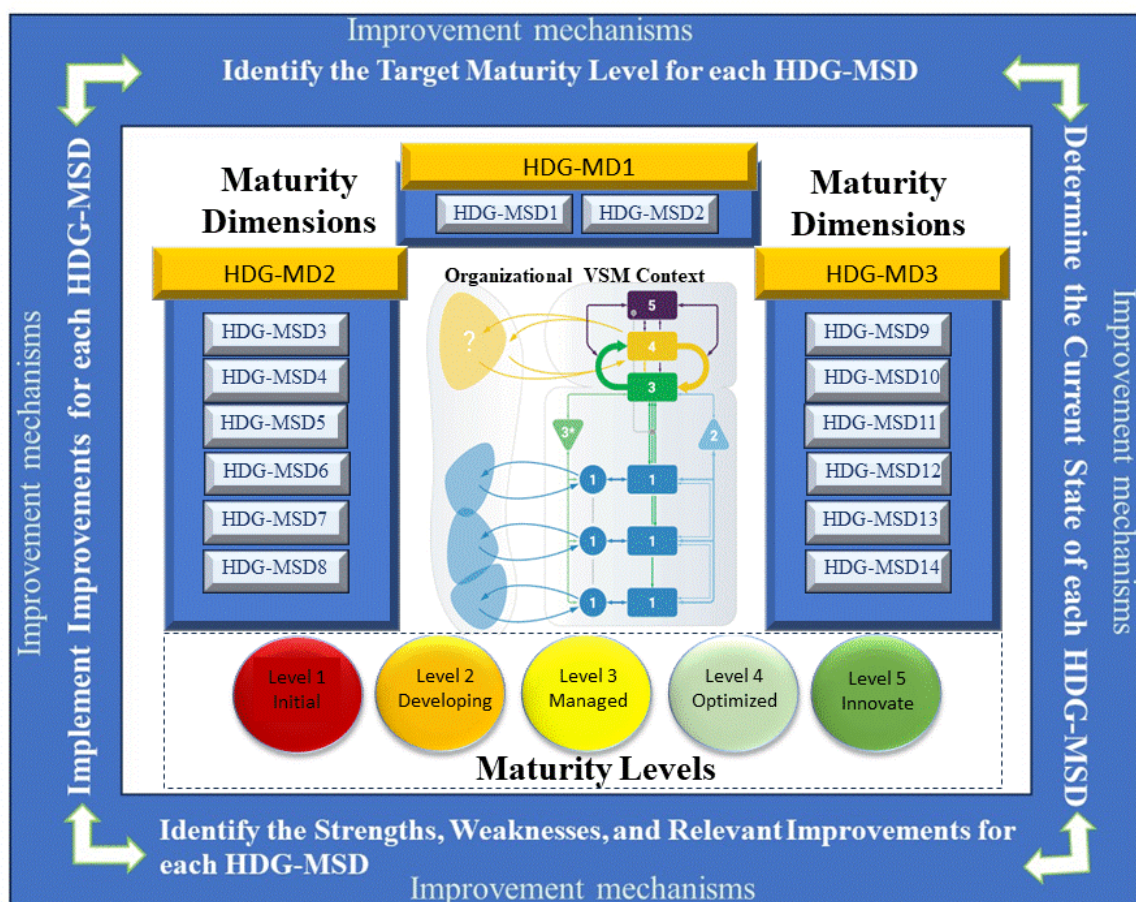
How many years of experience have you had in this current job?

How many years of experience in **Data/IT Governance**?

How many years of experience in the **Self-assessment model and matrix**?

How many years of experience in general governance?

Holistic Dark Data Governance Maturity Model



Evaluation criteria:

- **Completeness**

Please Rate the extent to which you agree or disagree with the following statements: 1= Strongly disagree 2= Disagree 3= Neutral 4= Agree 5= strongly agree		
Evaluating The Holistic Dark Data Governance Maturity Model Completeness		
Sub-criteria (code: MCMn)	Statement	Rating (1-5)
Scope (MCM1)	The model provides a maturity model for holistic dark data governance.	
Definition (MCM2)	The model clearly defined the maturity level for assessing the dimensions in the holistic dark data governance framework.	
Definitions (MCM3)	The model clearly defined dimensions in the holistic dark data governance model which requires assessing dark data governance systemic functions in the organisation.	
Definitions (MCM4)	The maturity levels have the right name to assess the dark data governance systemic functions in the organisation.	
Perceived Completeness (MCM5)	The dark data governance maturity model and assessment method are complete and recognizable as an adaptation of existing standards, models, and methods for holistic dark data governance.	

- **Consistency**

Please Rate the extent to which you agree or disagree with the following statements for 1= Strongly disagree 2= Disagree 3= Neutral 4= Agree 5= strongly agree		
Evaluating The Holistic Dark Data Governance Maturity Model Consistency		
Sub-criteria (Code: MICn)	Statement	Rating (1-5)

Internal Consistency (MIC1)	There is a consistent level of abstraction, granularity, and detail given within the holistic dark data governance maturity model.	

- Practicality**

Please rate the extent to which you agree or disagree with the following statements: 1= Strongly disagree 2= Disagree 3= Neutral 4= Agree 5= strongly agree		
Evaluate the Holistic Dark data governance maturity model practically		
Sub-criteria	Statement	Rating (1-5)
Easy to use	The holistic dark data governance maturity model is easy to use.	
Ease to learn	The holistic dark data governance maturity model is easy to learn.	
Understandable	The holistic dark data governance maturity model is simple to understand with its clearly defined systemic functions.	
Practical utility	The holistic dark data governance maturity model systemic functions provide utility for the organisation.	
Tailorable	The holistic dark data governance maturity model systemic functions are flexible, tailorable, and adaptable.	

- Usefulness**

Please rate the extent to which you agree or disagree with the following statements: 1= Strongly disagree 2= Disagree 3= Neutral 4= Agree 5= strongly agree		
Evaluating the Holistic Dark Data Governance Maturity Model Usefulness		
Sub-criteria (Code: MUSn)	Statement	Rating (1-5)
Perceived benefits (Code: MUS1)	The holistic dark data governance maturity model systemic functions are likely to be useful in assessing and improving the dark data governance holistic context in the organisation.	

Constructiveness (Code: MUS2)	The holistic dark data governance maturity model systemic functions are likely to be useful and benefit decision-makers in the organisation.	

• **Verifiability**

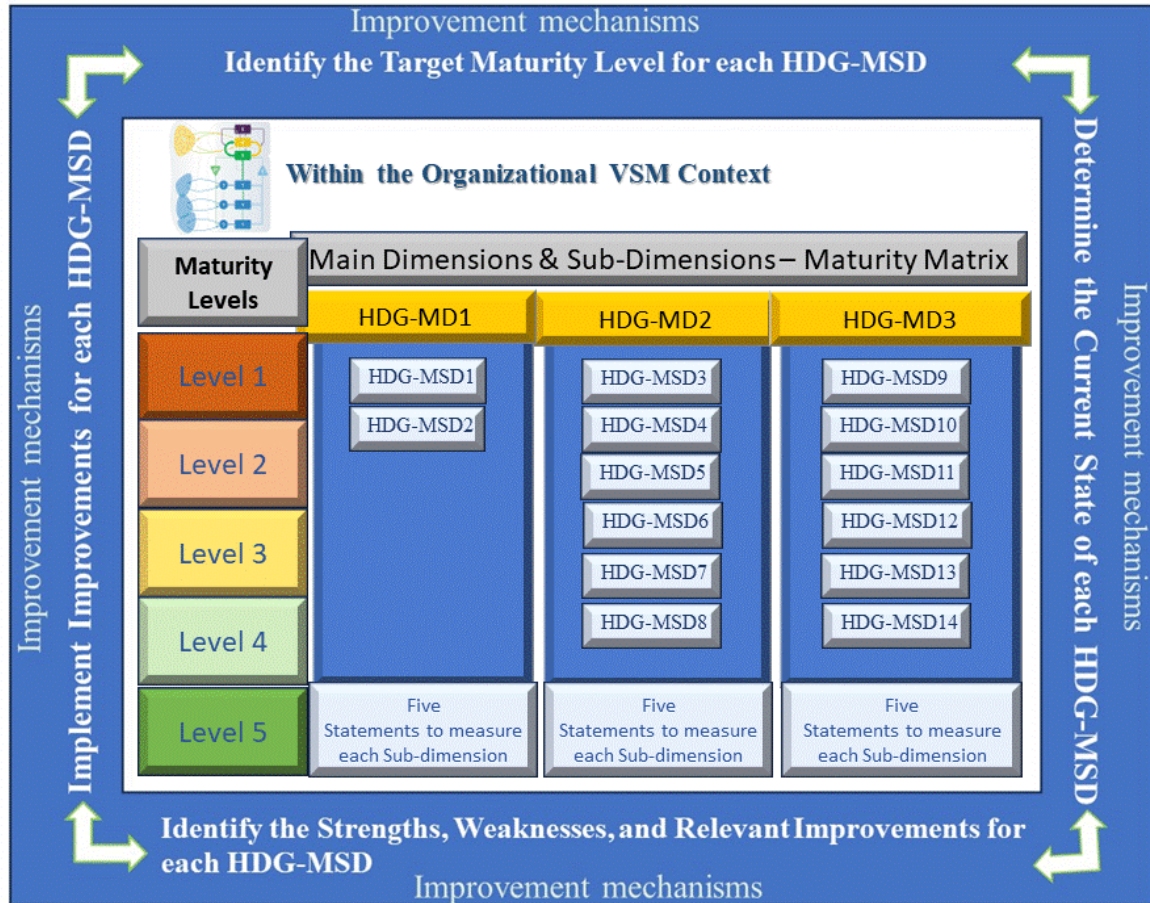
Please rate the extent to which you agree or disagree with the following statements: 1= Strongly disagree 2= Disagree 3= Neutral 4= Agree 5= strongly agree		
Evaluate The Holistic Dark Data Governance Maturity Model Verifiability		
Sub-criteria (Coded: MVRn)	Statement	Rating (1-5)
Feasible test coverage (MVR1)	The holistic dark data governance maturity model systemic functions meet their development objectives.	
Stability (MVR2)	The holistic dark data governance maturity model systemic functions in different organisations would produce consistent results patterns.	
Verifiable (MVR3)	The holistic dark data governance maturity model systemic functions can be verifiable	.

Could you please give your recommendations to update and improve the holistic dark data governance maturity model?

.....

Round 2 Questions

Holistic Dark Data Governance Assessment Matrix



The Conceptual Holistic Dark Data Governance Assessment Matrix

Details are described in Table 5.6, Table 5.7, and Table 5.8

Dimension /Level	Level 1	Level 2	Level 3	Level 4	Level 5
Dimension 1	Expectation-Dimension 1/ Level 1	Expectation-Dimension 1/ Level 2	Expectation-Dimension 1/ Level 3	Expectation-Dimension 1/ Level 4	Expectation-Dimension 1 /Level 5
Dimension 2	Expectation-Dimension 2/ Level 1	Expectation-Dimension 2 /Level 2	Expectation-Dimension 2/ Level 3	Expectation-Dimension 2 /Level 4	Expectation-Dimension 2/ Level 5
Dimension n	Expectation-Dimension n/ Level 1	Expectation-Dimension n/ Level 2	Expectation-Dimension n/ Level 3	Expectation-Dimension n/ Level 4	Expectation-Dimension n/ Level 5

Evaluation criteria:

- **Completeness**

Please rate the extent to which you agree or disagree with the following statements: 1= Strongly disagree 2= Disagree 3= Neutral 4= Agree 5= strongly agree		
Evaluating The Holistic Dark Data Governance Assessment Matrix Completeness		
Sub-criteria (Coded: ACM_n)	Statement	Rating (1-5)
Scope (ACM1)	The assessment matrix provides a tool to assess the holistic dark data governance in the organisation based on the holistic dark data governance maturity model structure.	
Definitions (ACM2)	The assessment matrix clearly defined the maturity level for assessing each dimension in the holistic dark data governance model.	
Definitions (ACM3)	The assessment matrix clearly defined the holistic dark data governance dimension's state at each level in the maturity model.	
Perceived Completeness (ACM4)	The holistic dark data governance assessment matrix is complete and recognizable as an adaptation of existing standards, models, and methods for holistic dark data governance.	

- **Consistency**

Please rate the extent to which you agree or disagree with the following statements: 1= Strongly disagree 2= Disagree 3= Neutral 4= Agree 5= strongly agree	

Evaluating The Holistic Dark Data Governance Assessment Matrix Consistency		
Sub-criteria (Code: AICn)	Statement	Rating (1-5)
Internal Consistency (AIC1)	There is a consistent level of abstraction, granularity, and detail given within the holistic dark data governance assessment matrix.	

- **Practicality**

Please rate the extent to which you agree or disagree with the following statements: 1= Strongly disagree 2= Disagree 3= Neutral 4= Agree 5= strongly agree		
Evaluating The Holistic Dark Data Governance Assessment Matrix Practicality		
Sub-criteria (Code: APR5)	Statement	Rating (1-5)
Ease of use (APR1)	The holistic dark data governance assessment matrix is easy to use.	
Ease to learn (APR2)	The holistic dark data governance maturity model is easy to learn.	
Understandable (APR3)	The holistic dark data governance assessment matrix is simple to understand with clearly defined systemic functions.	
Practical utility (APR4)	The holistic dark data governance assessment matrix systemic functions provide utility for the organisation.	
Tailorable (APR5)	The holistic dark data governance assessment matrix is flexible, tailorable, and adaptable.	

- **Usefulness**

Please rate the extent to which you agree or disagree with the following statements: 1= Strongly disagree 2= Disagree 3= Neutral 4= Agree 5= strongly agree		
Evaluating The Holistic Dark Data Governance Assessment Matrix Usefulness		
Sub-criteria (Code: AUSn)	Statement	Rating (1-5)
Perceived benefits (AUS1)	The holistic dark data governance assessment matrix is likely to be useful in assessing and improving the dark data governance systemic functions in the organisation.	
Constructiveness (AUS2)	The holistic dark data governance maturity model assessment matrix is likely to be useful and provide benefits to decision-makers in the organisation.	

- **Verifiability**

Please rate the extent to which you agree or disagree with the following statements: 1= Strongly disagree 2= Disagree 3= Neutral 4= Agree 5= strongly agree		
Evaluate The Holistic Dark Data Governance Assessment Matrix Verifiability		
Sub-criteria (Code: AVRn)	Statement	Rating (1-5)
Feasible test coverage (AVR1)	The holistic dark data governance assessment matrix meets its development objectives.	
Stability (AVR2)	The holistic dark data governance assessment matrix process in different organisations would produce consistent results patterns.	

Verifiable (AVR3)	The holistic dark data governance assessment matrix process can be verifiable.	

- **Strengths and Weaknesses**

Individual level in the Assessment Matrix		
Please rate the extent of your satisfaction with the following statements for evaluating the strengths and weaknesses of the holistic dark data governance assessment matrix: 1=Very Poor 2=Poor 3=Fair 4=Good 5= Very Good		
Evaluating The Strengths and Weaknesses of The Holistic Dark Data Governance Assessment Matrix: Individual level in assessment matrix (individual score) - Code: LC.n		
Sub-criteria	Statement	Rating (1-5)
LC.1	Level 1 in the assessment matrix provides strong content to measure the constructs of the holistic dark data governance maturity model.	
LC.2	Level 2 in the assessment matrix provides strong content to measure the constructs of the holistic dark data governance maturity model.	
LC.3	Level 3 in the assessment matrix provides strong content to measure the constructs of the holistic dark data governance maturity model.	
LC.4	Level 4 in the assessment matrix provides strong content to measure the constructs of the holistic dark data governance maturity model.	
LC.5	Level 5 in the assessment matrix provides strong content to measure the constructs of the holistic dark data governance maturity model.	

Could you please give your recommendations to update and improve the assessment matrix for holistic dark data governance?

.....

Round 3 Questions

- **Strengths and Weaknesses**

Individual Construct (Systemic Function)) in the Assessment Matrix		
Please rate the extent of your satisfaction with the following statements for evaluating the strengths and weaknesses of the holistic dark data governance assessment matrix: 1=Very Poor 2=Poor 3=Fair 4=Good 5= Very Good		
Evaluating The Strengths and Weaknesses of The Holistic Dark Data Governance Assessment Matrix: Individual construct in assessment matrix (individual score) – Code: DC.n		
Sub-criteria	Statement	Rating (1-5)
DC.1	The assessment matrix provides strong content to measure the “ HDG-MSD1: VSM Organisational Context and Goals ” construct in the holistic dark data governance maturity model for each maturity level.	
DC.2	The assessment matrix provides strong content to measure the “ HDG-MSD2: Identifying Recursive Organisational Level and HDG Scope ” construct in the holistic dark data governance maturity model for each maturity level.	

DC.3	The assessment matrix provides strong content to measure the “ HDG-MSD3: Deployment Context Systemic Functions (SF1) ” construct in the holistic dark data governance maturity model for each maturity level.	
DC.4	The assessment matrix provides strong content to measure the “ HDG-MSD4: Coordination Systemic Functions (SF2) ” construct in the holistic dark data governance maturity model for each maturity level.	
DC.5	The assessment matrix provides strong content to measure the “ HDG-MSD5: Control Systemic Functions (SF3) ” construct in the holistic dark data governance maturity model for each maturity level.	
DC.6	The assessment matrix provides strong content to measure the “ HDG-MSD6: Auditing and Compliance (SF3)* ” construct in the holistic dark data governance maturity model for each maturity level.	
DC.7	The assessment matrix provides strong content to measure the “ HDG-MSD7: Adaptation (SF4) ” construct in the holistic dark data governance maturity model for each maturity level.	
DC.8	The assessment matrix provides strong content to measure the “ HDG-MSD8: Strategic Direction and Feedback ” construct in the holistic dark data governance maturity model for each maturity level.	
DC.9	The assessment matrix provides strong content to measure the “ HDG-MSD9: Recursivity Levels Integration (SF6) ” construct in the holistic dark data governance maturity model for each maturity level.	
DC.10	The assessment matrix provides strong content to measure the “ HDG-MSD10: Requisite Variety Systemic Function (SF7) ” construct in the holistic dark data governance maturity model for each maturity level.	
DC.11	The assessment matrix provides strong content to measure the “ HDG-MSD11: Effective Inter-Operational Management (SF8) ” construct in the holistic dark data governance maturity model for each maturity level.	
DC.12	The assessment matrix provides strong content to measure the “ HDG-MSD12: Adaptability, Learning, and Change Management (SF9) ” construct in the holistic dark data governance maturity model for each maturity level.	

DC.13	The assessment matrix provides strong content to measure the “ HDG-MSD13: Communication Channels and Algedonic Channel (SF10) ” construct in the holistic dark data governance maturity model for each maturity level.	
DC.14	The assessment matrix provides strong content to measure the “ HDG-MSD14: Transduction and Integration of All Systems (SF11) ” construct in the holistic dark data governance maturity model for each maturity level.	

Could you please give your recommendations to update and improve the assessment matrix for holistic dark data governance?

.....

.....

.....

.....

.

Appendix P: Practical Evaluation Results – Recommendations for Improvements

➤ Case Scenario 1: University X

Given the size of University X and its diversity, holistic data governance is essential to ensuring organisational viability and aligning the institution's data governance strategy with its operational and strategic objectives. Below is the holistic data governance maturity assessment of University X across the 14 sub-dimensions (HDG-MSD1 to HDG-MSD14). This evaluation, conducted from the perspective of domain experts in data management, data governance, and executive management, assessed each sub-element and resulted in the following recommendations for improvements:

1. HDG-MSD1: VSM Organisational Context and Goals

- **Current Level: Level 3 (Managed/Proactive)**
 - **Analysis:** University X has a clear data governance structure, but alignment with the overall strategic business context is not fully optimized. Some processes are reactive, especially in addressing dark data, which is managed at an operational level rather than systemically. Holistic governance is recognized, but integration with long-term organisational goals is still evolving.
 - **Recommendation:** To reach Level 5 (Viable), University X should align its dark data governance goals fully with strategic objectives, ensuring predictive and proactive measures to support both operational and long-term institutional viability.

2. HDG-MSD2: Identifying Recursive Organisational Level and HDG Scope

- **Current Level: Level 2**
 - **Analysis:** There is a basic identification of data governance scope across the university's departments and schools, but the approach is fragmented, lacking systemic application across all-recursive levels of the institution. This limits the ability to consistently mitigate dark data risks.
 - **Recommendation:** Moving to Level 5 (Viable) requires the institution to define HDG scope at all organisational levels and integrate this with recursive business needs. Full organisation-wide alignment and real-time adjustments will ensure continuous support for strategic goals.

3. HDG-MSD3: Deployment Context Systemic Functions (SF1)

- **Current Level: Level 3**

- **Analysis:** Systemic functions are in place at University X, but dark data management remains inconsistent across business units, and the deployment is primarily operational rather than strategic.
- **Recommendation:** To progress to Level 5 (Viable), University X should ensure real-time deployment of systemic functions across all units using advanced tools and analytics, allowing the institution to continuously adjust based on evolving operational and strategic goals.

4. HDG-MSD4: Coordination Systemic Functions (SF2)

○ Current Level: Level 3

- **Analysis:** Coordination mechanisms exist, but their effectiveness varies across departments. Compliance with data governance policies is inconsistent, and conflicts are addressed reactively rather than pre-emptively.
- **Recommendation:** Moving to Level 5 (Viable) will require University X to adopt advanced predictive analytics and coordination mechanisms to anticipate conflicts and ensure full policy compliance across the university.

5. HDG-MSD5: Control Systemic Functions (SF3)

○ Current Level: Level 3

- **Analysis:** There are structured control mechanisms, but oversight is limited to specific departments, and there is no comprehensive control system across the institution.
- **Recommendation:** To reach Level 5 (Viable), the university should develop dynamic control mechanisms using automation and analytics that integrate across governance domains, ensuring continuous alignment with strategic objectives.

6. HDG-MSD6: Auditing and Compliance (SF3*)

○ Current Level: Level 2

- **Analysis:** While some auditing mechanisms exist, compliance evaluations are inconsistent, and auditing processes are often reactive rather than part of a systemic feedback loop. This limits University X's ability to use auditing for long-term governance improvements.
- **Recommendation:** For Level 5 (Viable), University X must establish systemic auditing and compliance mechanisms that provide real-time insights into data governance practices, driving continuous improvements and ensuring compliance with evolving regulations.

7. HDG-MSD7: Adaptation (SF4)

○ Current Level: Level 2

- **Analysis:** There are some mechanisms to address external changes, but dark data governance strategies are not consistently adapted to market or environmental changes. This reactive approach limits the institution's ability to support long-term viability.
- **Recommendation:** To achieve Level 5 (Viable), University X must implement predictive tools that enable proactive adaptation to external changes, ensuring that governance strategies continuously evolve in line with both operational needs and strategic goals.

8. HDG-MSD8: Strategic Direction and Feedback (SF5)

○ Current Level: Level 3

- **Analysis:** University X has a defined strategic direction for data governance, but feedback loops are not consistently applied across the institution. This results in a misalignment between current governance practices and long-term goals.
- **Recommendation:** To reach Level 5 (Viable), University X should establish continuous feedback mechanisms that align governance functions with both short-term and long-term organisational objectives, dynamically responding to changing requirements.

9. HDG-MSD9: Recursivity Levels Integration (SF6)

○ Current Level: Level 3

- **Analysis:** There is structured integration of governance domains at some levels of the institution, but this integration is not consistent across all-recursive levels. Dark data risks are managed at a departmental level, limiting the overall impact on organisational viability.
- **Recommendation:** To achieve Level 5 (Viable), University X should ensure that governance domains are fully integrated across all organisational levels, using continuous monitoring and analytics to support strategic alignment.

10. HDG-MSD10: Requisite Variety Systemic Function (SF7)

• Current Level: Level 2

- **Analysis:** Communication mechanisms are primarily reactive, with little focus on pre-emptively identifying external dark data threats. This reduces University X's ability to mitigate risks in real-time.
- **Recommendation:** Moving to Level 5 (Viable) requires University X to establish advanced communication channels that can dynamically respond to both internal and external data threats, ensuring resilience and long-term viability.

11. HDG-MSD11: Effective Inter-Operational Management (SF8)

• Current Level: Level 3

- **Analysis:** Interactions between HDG operational units and control functions exist but are inconsistent. Autonomy and synergy between departments are not fully optimized, limiting their ability to manage dark data risks effectively.
- **Recommendation:** To progress to Level 5 (Viable), University X should focus on predictive mechanisms that enhance synergy between operational units and real-time decision-making to improve data governance.

12. HDG-MSD12: Metasystem Adaptability, Learning, and Change Management (SF9)

- **Current Level: Level 2**

- **Analysis:** Basic change management processes exist, but they focus on short-term issues without fostering continuous learning and adaptability in data governance within the metasystem.
- **Recommendation:** To achieve Level 5 (Viable), University X must implement metasystem mechanisms for continuous learning and dynamic change management, enabling governance functions to evolve proactively based on feedback and changing external conditions.

13. HDG-MSD13: Communication Channels and Algedonic Channel (SF10)

- **Current Level: Level 3**

- **Analysis:** Communication channels exist, but they are not fully optimized for managing dark data risks dynamically. Algedonic channels for immediate feedback are underutilized.
- **Recommendation:** Moving to Level 5 (Viable) requires University X to develop fully adaptive communication systems that allow real-time responses to high dark data risk scenarios and adequate responses for other risk scenarios, enhancing operational efficiency and strategic alignment.

14. HDG-MSD14: Transduction and Integration of All Systems (SF11)

- **Current Level: Level 3**

- **Analysis:** Transduction processes exist but are not fully integrated across all systemic functions. Siloed data governance limits knowledge sharing across departments.
- **Recommendation:** To reach Level 5 (Viable), University X should create fully adaptive transduction processes that ensure cohesive operations and shared knowledge across all systemic functions, reducing silos and improving organisational viability.

➤ Case Scenario 2: University Y

University Y is a leading public research institution with a large and diverse community of faculty, staff, and students. With its size and scope, ensuring robust and holistic data

governance across all departments and governance domains (Data, IT, Corporate) is essential for supporting organisational viability, operational efficiency, and long-term strategic goals.

Below is an assessment of University Y's holistic data governance maturity across the 14 sub-dimensions (HDG-MSD1 to HDG-MSD14). This evaluation, conducted from the perspective of domain experts in data management, data governance, and executive management, assessed each sub-element and resulted in the following recommendations for improvements:

1. HDG-MSD1: VSM Organisational Context and Goals

- **Current Level:** Level 3 (Managed/Proactive)
 - **Analysis:** University Y has a structured data governance strategy that is aligned with the institution's business objectives, though there are some reactive elements, particularly in the handling of dark data. The institution focuses on compliance and regulatory aspects, but the holistic integration of governance across all departments and functions is still evolving.
 - **Recommendation:** To reach Level 5 (Viable), the university needs to ensure continuous alignment between its dark data governance goals and long-term strategic objectives. Predictive tools and proactive governance should be implemented to enhance adaptability and organisational viability.

2. HDG-MSD2: Identifying Recursive Organisational Level and HDG Scope

- **Current Level:** Level 2 (Developing/Defined)
 - **Analysis:** The university has identified some elements of HDG scope but has yet to apply a comprehensive approach that integrates governance across all recursive organisational levels (from departments to the central administration). Dark data governance scope is inconsistent across units.
 - **Recommendation:** To reach Level 5 (Viable), University Y must define the HDG scope across all levels of the organisation and ensure that governance is aligned with both business and operational needs. This requires organisation-wide integration with real-time adaptability.

3. HDG-MSD3: Deployment Context Systemic Functions (SF1)

- **Current Level:** Level 3 (Managed/Proactive)
 - **Analysis:** Systemic functions of HDG are implemented in some areas, especially in IT and data compliance. However, these functions are not fully integrated into all business units. Governance practices are not consistently aligned across all organisational layers, limiting the proactive management of dark data risks.
 - **Recommendation:** To progress to Level 5 (Viable), University Y should implement predictive tools and deploy systemic functions organisation-wide, allowing real-time adjustments based on operational and strategic shifts.

4. HDG-MSD4: Coordination Systemic Functions (SF2)

- **Current Level:** Level 2 (Developing/Defined)
 - **Analysis:** Coordination between governance domains is improving, but dark data governance policies are not fully enforced across all departments. Compliance remains reactive, and conflicts related to data handling are typically addressed after they occur.
 - **Recommendation:** To achieve Level 5 (Viable), University Y must adopt predictive coordination mechanisms that ensure compliance with governance policies and prevent conflicts across departments. This can be accomplished by integrating advanced analytics and creating alignment with corporate strategies.

5. HDG-MSD5: Control Systemic Functions

- **Current Level:** Level 2 (Developing/Defined)
 - **Analysis:** Basic control mechanisms exist, primarily within IT governance, but these are inconsistent and fragmented across business units. There is little integration between control functions and other governance domains, limiting the university's ability to mitigate risks holistically.
 - **Recommendation:** To reach Level 5 (Viable), University Y must enhance its control functions by integrating them across all governance domains (e.g., IT, data, and corporate governance). Advanced automation and monitoring systems should be implemented to ensure continuous alignment with business goals.

6. HDG-MSD6: Auditing and Compliance (SF3)

- **Current Level:** Level 2 (Developing/Defined)
 - **Analysis:** While some auditing mechanisms are in place, compliance evaluations are inconsistent, and there is limited use of audits to inform data governance improvements. The current approach lacks real-time compliance tracking, which limits its ability to support organisational viability.
 - **Recommendation:** To move to Level 5 (Viable), University Y must establish systematic and dynamic auditing processes, utilizing predictive analytics to provide continuous compliance insights. This will support long-term organisational improvements and ensure alignment with evolving regulations.

7. HDG-MSD7: Adaptation (SF4)

- **Current Level:** Level 2 (Developing/Defined)
 - **Analysis:** University Y has started addressing external changes, but its governance strategies are largely reactive. The institution lacks a formal, proactive framework for adapting governance to market trends and regulatory shifts, which limits its long-term adaptability.
 - **Recommendation:** To reach Level 5 (Viable), the university needs to integrate predictive tools that support continuous learning and adaptability. Governance strategies should be dynamic and able to adjust to both external and internal changes in real time.

8. HDG-MSD8: Strategic Direction and Feedback

- **Current Level:** Level 3 (Managed/Proactive)
 - **Analysis:** Strategic direction for data governance is defined but not consistently applied across all units. Feedback loops exist, but they are not fully utilized to align governance practices with both current and future states, limiting the long-term strategic alignment.
 - **Recommendation:** To reach Level 5 (Viable), University Y should establish continuous feedback mechanisms that inform governance practices and ensure dynamic alignment with both short-term and long-term strategic goals.

9. HDG-MSD9: Recursivity Levels Integration (SF6)

- **Current Level:** Level 2 (Developing/Defined)
 - **Analysis:** Integration of governance domains at different recursive organisational levels is limited. Dark data challenges are addressed reactively, and there is minimal coordination across departments to ensure a comprehensive governance approach.
 - **Recommendation:** To reach Level 5 (Viable), University Y must ensure full integration of governance domains across all recursive levels of the organisation. This involves continuous monitoring and alignment with both operational needs and strategic objectives.

10. HDG-MSD10: Requisite Variety Systemic Function (SF7)

- **Current Level:** Level 2 (Developing/Defined)
 - **Analysis:** Communication channels exist but are reactive in addressing dark data risks. The university has limited mechanisms for proactively managing external threats, and there is little coordination between business units regarding these risks.
 - **Recommendation:** To progress to Level 5 (Viable), University Y must develop proactive communication mechanisms supported by predictive analytics to enable real-time responses to external data threats. This will ensure organisational resilience and improve risk mitigation.

11. HDG-MSD11: Effective Inter-Operational Management (SF8)

- **Current Level:** Level 3 (Managed/Proactive)
 - **Analysis:** University Y has established interactions between operational units, but these interactions are not fully optimized for synergy. While some coordination exists, there is limited autonomy for units to manage their governance functions independently and efficiently.
 - **Recommendation:** To move to Level 5 (Viable), the university must enhance the synergy between operational units by implementing predictive tools that provide real-time insights and allow for autonomous decision-making.

12. HDG-MSD12: Metasystem Adaptability, Learning, and Change Management (SF9)

- **Current Level:** Level 2 (Developing/Defined)
 - **Analysis:** Change management processes focus on short-term adaptations, and there is little emphasis on continuous learning or adaptability in governance practices. This limits the university's ability to evolve its data governance strategies in response to internal and external challenges.
 - **Recommendation:** To reach Level 5 (Viable), University Y should implement continuous learning mechanisms and a dynamic change management framework that enables governance practices to evolve based on real-time feedback and strategic needs.

13. HDG-MSD13: Communication Channels and Algedonic Channel (SF10)

- **Current Level:** Level 3 (Managed/Proactive)
 - **Analysis:** University Y has communication channels in place, but these are not fully optimized for managing dark data risks dynamically. Algedonic channels are underutilized, reducing the university's ability to respond rapidly to high-risk scenarios.
 - **Recommendation:** To reach Level 5 (Viable), University Y must develop fully adaptive communication systems that enable real-time interventions in high-risk scenarios, ensuring better alignment with strategic goals.

14. HDG-MSD14: Transduction and Integration of All Systems (SF11)

- **Current Level:** Level 3 (Managed/Proactive)
 - **Analysis:** Transduction processes exist, but the integration of governance systems across all functions is incomplete. There is limited sharing of knowledge between data and business stakeholders, creating silos that undermine comprehensive governance.
 - **Recommendation:** To progress to Level 5 (Viable), University Y must develop fully adaptive transduction processes that ensure the seamless integration of governance functions and knowledge-sharing across all departments, reducing silos and supporting organisational viability.

➤ Case Scenario 3: University Z

University Z is a large public research university with a diverse range of academic programs and a large faculty, staff, and student body. Managing data governance effectively in such a vast institution is crucial to supporting its operational and strategic goals. This assessment evaluates University Z's holistic data governance maturity across the 14 sub-dimensions (HDG-MSD1 to HDG-MSD14). This evaluation, conducted from the perspective of domain experts in data management, data governance, and executive management, assessed each sub-element and resulted in the following recommendations for improvements:

1. HDG-MSD1: VSM Organisational Context and Goals

- **Current Level:** Level 2 (Developing/Defined)
 - **Analysis:** University Z has started to develop data governance goals, but they are not consistently aligned with the university's strategic objectives. The approach is still informal, with limited focus on long-term planning or alignment with business goals.
 - **Recommendation:** To move to Level 5 (Viable), University Z needs to establish clear dark data governance goals that are fully integrated with the institution's business and academic objectives, using predictive tools to ensure alignment and support for organisational viability.

2. HDG-MSD2: Identifying Recursive Organisational Level and HDG Scope

- **Current Level:** Level 2 (Developing/Defined)
 - **Analysis:** While there is some recognition of the need to define HDG scope across departments, the approach remains fragmented. Governance practices are not yet aligned at all recursive levels, limiting the institution's ability to consistently manage dark data risks.
 - **Recommendation:** To progress to Level 5 (Viable), the university should implement a comprehensive HDG scope across all levels and ensure real-time alignment with both business and operational needs.

3. HDG-MSD3: Deployment Context Systemic Functions (SF1)

- **Current Level:** Level 3 (Managed/Proactive)
 - **Analysis:** The systemic functions of HDG are deployed in certain areas, especially IT and compliance. However, they are inconsistently applied across the institution, limiting the full potential of data governance to mitigate risks and create business value.
 - **Recommendation:** To reach Level 5 (Viable), University Z needs to deploy systemic functions across all departments and ensure that real-time adjustments are made to continuously align governance with operational and strategic goals.

4. HDG-MSD4: Coordination Systemic Functions (SF2)

- **Current Level:** Level 2 (Developing/Defined)
 - **Analysis:** There are basic coordination mechanisms in place, but enforcement and alignment with corporate policies are inconsistent. As a result, there is minimal impact on ensuring compliance and mitigating conflicts related to data governance.
 - **Recommendation:** To move to Level 5 (Viable), the university must implement advanced coordination mechanisms that allow for predictive management of conflicts and ensure compliance with data governance policies across all departments.

5. HDG-MSD5: Control Systemic Functions

- **Current Level:** Level 3 (Managed/Proactive)
 - **Analysis:** University Z has structured control mechanisms in place, particularly in IT and compliance. However, these control functions are not fully integrated

with other governance domains, leading to gaps in oversight and the holistic management of risks.

- **Recommendation:** To reach Level 5 (Viable), University Z must integrate control mechanisms across all governance domains, using automation and advanced analytics to ensure real-time monitoring and alignment with strategic objectives.

6. HDG-MSD6: Auditing and Compliance (SF3)

- **Current Level:** Level 2 (Developing/Defined)
 - **Analysis:** Basic auditing processes are in place, but compliance evaluations are inconsistent. Audit results are not used systematically to inform improvements in data governance practices, which limits the university's ability to manage risks effectively.
 - **Recommendation:** For Level 5 (Viable), University Z should implement a systematic auditing and compliance framework, supported by real-time data and analytics, to provide continuous insights into governance practices and drive improvements.

7. HDG-MSD7: Adaptation (SF4)

- **Current Level:** Level 2 (Developing/Defined)
 - **Analysis:** The university has made some progress in adapting to external changes, but governance strategies are still largely reactive. There is no formal process for continuously adapting governance based on market trends or regulatory changes.
 - **Recommendation:** To move to Level 5 (Viable), University Z needs to implement predictive tools that support the continuous adaptation of governance strategies in response to external changes, ensuring that data governance remains aligned with both operational and strategic needs.

8. HDG-MSD8: Strategic Direction and Feedback

- **Current Level:** Level 3 (Managed/Proactive)
 - **Analysis:** Strategic direction for data governance has been established, but feedback loops are inconsistently applied. This leads to misalignments between governance practices and the institution's long-term goals.
 - **Recommendation:** To reach Level 5 (Viable), University Z should develop continuous feedback mechanisms that ensure real-time adjustments to governance practices, keeping them aligned with both short-term and long-term objectives.

9. HDG-MSD9: Recursivity Levels Integration (SF6)

- **Current Level:** Level 2 (Developing/Defined)
 - **Analysis:** Integration of governance domains across recursive organisational levels is still limited. Dark data risks are managed inconsistently across departments, which weakens the overall impact of governance efforts on organisational viability.

- **Recommendation:** To progress to Level 5 (Viable), University Z must ensure full integration of governance domains at all organisational levels, supported by continuous monitoring and real-time adjustments to align governance with strategic goals.

10. HDG-MSD10: Requisite Variety Systemic Function (SF7)

- **Current Level:** Level 2 (Developing/Defined)
 - **Analysis:** Communication channels exist, but they are primarily reactive. The university has not yet developed effective mechanisms for proactively identifying and managing external dark data threats, which limits the university's ability to mitigate risks in real-time.
 - **Recommendation:** To reach Level 5 (Viable), University Z must implement proactive communication channels supported by predictive analytics to dynamically manage external threats and ensure resilience.

11. HDG-MSD11: Effective Inter-Operational Management (SF8)

- **Current Level:** Level 3 (Managed/Proactive)
 - **Analysis:** There are defined interactions between operational units, but they are not fully synergized. Autonomy and control within units are not balanced effectively, which limits the university's ability to optimize its decision-making processes.
 - **Recommendation:** To reach Level 5 (Viable), University Z should enhance synergy between operational units using predictive tools that provide real-time insights, enabling more autonomous decision-making and improved governance outcomes.

12. HDG-MSD12: Metasystem Adaptability, Learning, and Change Management (SF9)

- **Current Level:** Level 2 (Developing/Defined)
 - **Analysis:** The university's change management processes focus on short-term issues, with limited emphasis on adaptability and continuous learning in data governance. This restricts the ability to evolve governance strategies in response to emerging challenges.
 - **Recommendation:** To progress to Level 5 (Viable), University Z should implement continuous learning mechanisms and a dynamic change management framework that enables governance practices to evolve based on real-time feedback and external changes.

13. HDG-MSD13: Communication Channels and Algedonic Channel (SF10)

- **Current Level:** Level 3 (Managed/Proactive)
 - **Analysis:** Communication channels for addressing dark data risks exist but are not fully adaptive. Algedonic channels are underutilized, resulting in slower responses to high-risk scenarios.
 - **Recommendation:** To reach Level 5 (Viable), University Z should develop fully adaptive communication networks that allow for real-time intervention in high-risk situations, ensuring that governance practices are dynamically aligned with strategic objectives.

14. HDG-MSD14: Transduction and Integration of All Systems (SF11)

- **Current Level:** Level 3 (Managed/Proactive)
 - **Analysis:** Transduction processes are established, but integration across all governance functions is incomplete. Silos exist between departments, limiting the sharing of data governance knowledge and practices.
 - **Recommendation:** To progress to Level 5 (Viable), University Z should focus on creating fully adaptive transduction processes that promote seamless integration across governance systems and reduce organisational silos.