

**AN INTEGRATED CYBERSECURITY RISK MANAGEMENT (I-  
CSRM) FRAMEWORK FOR CRITICAL INFRASTRUCTURE  
PROTECTION**

**Halima Ibrahim Kure**

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

March 2021

## **Dedication**

To my parents (AVM Ibrahim Abdullahi Kure and Mrs Adama Kure), my children (Halima Hanan and Ibrahim Khalilullah Etsu-Ndagi) and my siblings (Siyama, Abdullahi, Sa'adatu and Nana Kure) without whom this research wouldn't have been possible.

## **Acknowledgement**

The researcher would like to acknowledge and recognise several professionals whose significant efforts made this study possible. Others are family and colleagues who have helped me during my studies. From an academic standpoint, I am grateful to my wonderful supervisor, Dr Shareeful Islam, for leading me through this research project with informative insights, advice, input, inspiration, and support.

I would also like to thank Dr Mustansar Ghazanfar and Dr Aloysius Edoh for their study assistance. I would also like to express my heartfelt gratitude to the Commandant (Nigerian Defence Academy) for providing me with the opportunity to pursue a PhD in Computing, to NDA TETFUND for providing me with the initial scholarship to begin my degree, and to PTDF for taking on responsibility for the remainder of my studies. I would also like to thank Distribution Companies (DisCos) Nigeria for giving me the chance to evaluate my research. A million thanks also go out to the case-study organisation's stakeholders, who helped me carry out my analysis and provide helpful feedback.

I want to express my most profound appreciation and respect to my brother Dr Umar Isma'il Mukhtar, who stood by me through all of my trials and tribulations, making enormous sacrifices to ensure that my PhD is achieved. Also, I would also like to thank Aunty Nana and Uncle Musa for their invaluable assistance. A special thanks to my friends Nawa Augustine and Ahmed Galadima for taking me through some programming classes and guiding me.

## ABSTRACT

Risk management plays a vital role in tackling cyber threats within the Cyber-Physical System (CPS) for overall system resilience. It enables identifying critical assets, vulnerabilities, and threats and determining suitable proactive control measures to tackle the risks. However, due to the increased complexity of the CPS, cyber-attacks nowadays are more sophisticated and less predictable, which makes risk management task more challenging. This research aims for an effective Cyber Security Risk Management (CSRM) practice using assets criticality, predication of risk types and evaluating the effectiveness of existing controls. We follow a number of techniques for the proposed unified approach including fuzzy set theory for the asset criticality, machine learning classifiers for the risk predication and Comprehensive Assessment Model (CAM) for evaluating the effectiveness of the existing controls.

The proposed approach considers relevant CSRM concepts such as threat actor attack pattern, Tactic, Technique and Procedure (TTP), controls and assets and maps these concepts with the VERIS community dataset (VCDB) features for the purpose of risk predication. Also, the tool serves as an additional component of the proposed framework that enables asset criticality, risk and control effectiveness calculation for a continuous risk assessment. Lastly, the thesis employs a case study to validate the proposed i-CSRM framework and i-CSRMT in terms of applicability. Stakeholder feedback is collected and evaluated using critical criteria such as ease of use, relevance, and usability. The analysis results illustrate the validity and acceptability of both the framework and tool for an effective risk management practice within a real-world environment.

The experimental results reveal that using the fuzzy set theory in assessing assets' criticality, supports stakeholder for an effective risk management practice. Furthermore, the results have demonstrated the machine learning classifiers' have shown exemplary performance in predicting different risk types including denial of service, cyber espionage, and Crimeware. An accurate prediction can help organisations model uncertainty with machine learning classifiers, detect frequent cyber-attacks, affected assets, risk types, and employ the necessary corrective actions for its mitigations.

Lastly, to evaluate the effectiveness of the existing controls, the CAM approach is used, and the result shows that some controls such as network intrusion, authentication, and anti-virus show high efficacy in controlling or reducing risks. Evaluating control effectiveness helps organisations to know how effective the controls are in reducing or preventing any form of risk before an attack occurs. Also, organisations can implement new controls earlier. The main advantage of using the CAM approach is that the parameters used are objective, consistent and applicable to CPS.

## Table of Contents

Acknowledgement .....	3
List of Tables .....	10
List of Figures .....	12
List of Abbreviations .....	15
CHAPTER ONE .....	16
1. Introduction .....	16
1.2. Statement of the Problem .....	17
1.3. Research Questions.....	19
1.4. Research Aim and Objectives.....	20
1.6. Empirical Evaluation .....	22
1.8. Chapter Summary .....	24
CHAPTER TWO .....	25
Background and Literature Review .....	25
2.1. Introduction.....	25
2.1. Overview of Critical Infrastructure Systems .....	25
2.2. Critical Infrastructure Domains .....	27
2.2.1. Healthcare Infrastructure.....	28
2.2.2. Power Grid Infrastructure.....	28
2.2.3. Transport Infrastructure.....	29
2.2.4. Financial Infrastructure .....	30
2.2.5. Telecommunication Networks .....	30
2.2.6. Software Development Projects .....	30
2.3. Critical Infrastructure Interdependency .....	31
2.3.1. Interdependency of Critical infrastructure Domains .....	32
2.3.2. Asset Interdependency within a Critical Infrastructure Domain .....	32
2.3.3. Cascading Impact/effect.....	33
2.4. Risk Assessment Overview .....	34
2.4.1. Need for Risk Assessment in Critical Infrastructure .....	36
2.4.2. Risk Management methodologies for Critical Infrastructure .....	37
2.4.3. Cyber Threat Intelligence (CTI).....	38
2.4.4. Threat Taxonomy .....	39
2.5.1. Risk Management in Critical Infrastructure .....	42
2.5.2. Frameworks/Standards/models for critical infrastructure .....	45
2.5.3. Machine learning Technique for Risk prediction.....	46
2.5.4. Case Study.....	50
2.6. Challenges faced by critical infrastructure systems.....	52
2.6.1. Evolving Cyber-threat landscape .....	53
2.6.2. Adopting Machine Learning Techniques .....	54

<b>2.7. Summary</b> .....	55
CHAPTER THREE .....	56
3.1. Introduction.....	56
<b>3.2. Methodology for Framework Development</b> .....	57
3.2.1. Step 1: Literature Review.....	58
3.2.2. Step 2: Development of Framework and Process.....	59
3.2.3. Step 3: Research Validation .....	61
3.3. Research Approach.....	61
3.3.1. Qualitative research approach .....	62
3.3.2. Quantitative research approach .....	62
3.3.3. Mixed Research Approach .....	62
3.4. Adopted Research method by this research.....	62
3.5. Research Design .....	63
3.6. Research Strategy .....	65
3.7. Action Research.....	66
3.8. Case Study .....	67
3.9. Data collection methods .....	67
3.9.1. Interviews.....	68
3.9.2. Informal Meetings/Workshops.....	68
3.9.3. Observation .....	68
3.9.4. Documentation .....	68
3.9.5. Experiments.....	69
3.11. Expert Opinion .....	69
3.12. Summary.....	86
Integrated Cybersecurity Risk Management (i-CSRМ) Framework .....	69
4.1. Introduction.....	<b>Error! Bookmark not defined.</b>
4.3. Conceptual View of i-CSRМ .....	71
<b>4.3.1. Actor</b> .....	72
4.3.2. Assets .....	73
4.3.3. Goals .....	75
4.3.4. Threat Actor .....	77
4.3.5. TTP.....	78
4.3.6. Indicator of Compromise .....	79
4.3.7. Vulnerability.....	80
4.3.8. threat.....	80
4.3.9. Risk .....	81
4.3.10. Controls .....	82
CHAPTER FIVE .....	88
Process for the Integrated Cybersecurity Risk Management (i-CSRМ) Framework.....	88

5.1. Introduction.....	88
5.2. Integrated Cybersecurity Risk Management Process: A Unified Approach .....	88
5.2.1. Cyber Threat Intelligence (CTI).....	89
5.2.2. Fuzzy logic .....	89
5.2.3. Risk Management Standards .....	89
5.2.4. Controls .....	90
5.3. Integrated Cybersecurity Risk Management (i-CSRMT) Process .....	91
5.3.1. Activity 1: Organisational context .....	94
5.3.2. Activity 2: Asset Identification and Criticality .....	94
5.3.3. Activity 3: Threat Modelling.....	100
5.3.4 Activity 4: Risk Assessment .....	105
5.3.5 Activity 5: Risk Controls.....	109
CHAPTER SIX.....	113
Integrated Cybersecurity Risk Management Tool (i-CSRMT).....	113
6.1. Introduction.....	113
6.2. Overview of i-CSRMT .....	113
6.3. General Description of i-CSRMT Tool .....	114
6.4. Design process.....	114
6.5. Architecture of i-CSRMT .....	115
6.5.1. Presentation Layer.....	115
6.5.2. Application Layer.....	115
6.5.3. Database Layer .....	115
6.6. I-CSRMT Features .....	116
6.7. Dashboard Views.....	117
6.7.1. Super Administrator Dashboard.....	118
6.7.2. Company Administrator Dashboard.....	120
6.7.3. Identification of Actors and Role Dashboard.....	122
6.7.4. Managing Project Dashboard .....	124
CHAPTER SEVEN .....	<b>Error! Bookmark not defined.</b>
Evaluation of i-CSRMT Framework.....	130
7.1. Introduction.....	<b>Error! Bookmark not defined.</b>
7.2. Empirical Research method.....	131
7.2.1. Data collection.....	132
7.3. Dataset Description: Implementation of Machine learning classifiers for Risk prediction.....	133
7.3.1. Mapping .....	133
7.3.1. Experimental Setup .....	136
7.3.2. Feature Extraction .....	136
7.3.3. Features and classification labels .....	137
7.3.4. Classification.....	140

7.3.5. Training the machine learning classifiers.....	140
7.3.6. Evaluation measures.....	142
7.4. Case study: Implementation of i-CSR Framework .....	142
7.4.1. Study context.....	142
7.4.2. The Workflow .....	143
7.4.3. Recent Cyber Incident.....	143
7.5. Implementation of i-CSR for the Study Context.....	144
7.5.1. Activity 1: Organisational Context.....	145
7.5.2. Activity 2: Asset Identification and Criticality .....	147
7.5.3. Activity 3: Threat Modelling.....	154
7.5.4. Activity 4: Risk Assessment .....	156
7.5.5. Activity 5: Risk Controls.....	164
7.6.1. Ease of Use Parameter.....	169
7.6.2 Relevance Parameter .....	170
7.6.3. Usefulness Parameter .....	170
7.6.4. Flexibility Parameter .....	171
7.8. Summary of the Chapter.....	173
CHAPTER 8 .....	175
DISCUSSION .....	175
8. Introduction.....	175
8.1. Comparison between i-CSR Framework with other Works.....	175
8.2. Criteria for Reference Comparison.....	175
8.3. Discussion on Comparison Findings .....	177
8.3.1. Tool Support.....	177
8.3.2. Conceptualization of Cybersecurity Risk Management .....	177
8.3.3. Adoption of Industry Standards .....	178
8.3.4. Integration of machine learning techniques for i-CSR findings on Dataset .....	179
8.3.5. Implementation process.....	181
8.4. Discussion about case study findings .....	182
8.4.1. Applicability of the Framework on case study.....	182
8.4.2. Comparison with Existing Study Results.....	183
8.4.3. Study Limitation and Validity.....	184
8.5. Integrating CTI with i-CSR findings.....	185
8.5.1. Applicability of CTI for improving i-CSR .....	185
8.5.2. The result from the case study.....	186
8.5.3. comparison with other work in adopting CTI for risk management .....	186
8.6. Empirical Studies Conclusion.....	187
8.7. Summary .....	187
CHAPTER NINE.....	189

Conclusion and Further Research .....	<b>Error! Bookmark not defined.</b>
9.1. Introduction.....	189
9.2. Fulfilling Research Objectives .....	189
9.2.1. Develop a Novel Framework .....	190
9.2.2. Propose i-CSRMT process .....	191
9.2.3. Integration of automated techniques for the prediction of risk level.....	192
9.2.4. To evaluate the effectiveness of existing controls.....	192
9.2.5. Develop i-CSRMT .....	192
9.2.6. Validate i-CSRMT in real-life critical infrastructure sectors .....	193
9.3. Research Limitation.....	193
9.4. Further Research.....	194
9.5. Summary.....	195
References.....	197
Appendices.....	215
Appendix A: Questionnaire Evaluation for Framework Evaluation .....	215

## List of Tables

Table 4.1: Relationship between Concepts .....	86
Table 5.1: i-CSR Framework Process .....	92
Table 5.2: Fuzzy Ratings .....	97
Table 5.3: Asset Inventory .....	223
Table 5.4: Vulnerability Factor Rating .....	101
Table 5.5: Threat Actor Factors Rating .....	102
Table 5.6: TTP and IOC (Tactic, 2017) .....	103
Table 5.7: Threat Profile .....	224
Table 5.8: Overall Likelihood Rating .....	107
Table 5.9: Impact Factors .....	108
Table 5.10: Overall Impact <sub>F</sub> Rating .....	108
Table 5.11: Overall Risk level .....	109
Table 5.12: Control Types .....	225
Table 5.13: Criteria Rating .....	110
Table 5.14: Overall effectiveness.....	111
Table 5.15: Risk Control Profile.....	225
Table 5.16: Risk status.....	225
Table 5.17: Risk Register.....	226
Table 7.1: Summary of Responses from researched case-study .....	132
Table 7.2: Feature vector for threat actor for VCDB dataset.....	134
Table 7.3: Feature vector for asset for VCDB dataset .....	135
Table 7.4: Feature vector TTP for VCDB dataset.....	135
Table 7.5: Feature vector for control for VCDB dataset.....	136
Table 7.6: Feature vector as output features for control for VCDB dataset.....	137
Table 7.7: Threat Actor type feature detail.....	138
Table 7.8: Asset type feature detail .....	138
Table 7.9: Asset type feature detail .....	138
Table 7.10: TTP type feature detail.....	139
Table 7.11: Feature vector weights.....	139
Table 7.12: Classification Models and feature description.....	140
Table 7.13: Notations used for building the classifier.....	141
Table 7.14: List of Actors and their Roles .....	145
Table 7.15: Assets Identification .....	148
Table 7.16: Asset criticality results.....	153
Table 7.17: Performance of the features on each of the classifiers for predicting risk types.....	157

Table 7.18: Performance measure for KNN classifier for the various risk types based on the different features.....	<b>Error! Bookmark not defined.</b>
Table 7.19: Existing Control Types .....	165
Table 7.20: Responses from received from Case-Study .....	169
Table 7.21: Stakeholders' Perception of i-CSR Framework's Ease of Use .....	170
Table 7.21: Framework's relevance for supporting the organisations achieve risk management .....	170
Table 7.22: Responses on the Usefulness of i-CSR Framework .....	171
Table 7.23: Responses on the Flexibility of i-CSR Framework.....	171
Table 7.24: Rating on Framework's compliance with relevant laws, standards and best practices ...	172
Table 7.25: Responses on the Trustworthiness of i-CSR Framework.....	172
Table 8.1: Comparison Parameters .....	176

## List of Figures

Figure 1.1: Overview of thesis structure.....	24
Figure 2.1: An overview of the Power Grid System.....	29
Figure 2.2: Interdependency of Assets.....	33
Figure 2.3: Threat, vulnerability, countermeasures and asset relationship (Jenkins, 1998).....	35
Figure 3.1: Research Methodology.....	<b>Error! Bookmark not defined.</b>
Figure 3.2: Summary of Research Design.....	65
Figure 3.3: Evaluation process of the proposed framework.....	67
Figure 4.1: Unified approach model.....	71
Figure 4.2: Actors Classification.....	73
Figure 4.3: Asset Classification.....	75
Figure 4.4: Goal Classification.....	77
Figure 4.5: Threat Actor Classification.....	77
Figure 4.6: TTP classification.....	78
Figure 4.7: Indicators of Compromise Classification.....	79
Figure 4.8: Vulnerability Classification.....	80
Figure 4.9: Threat Classification.....	81
Figure 4.10: Risk Classification.....	82
Figure 4.11: Control Classification.....	83
Figure 4.12: Overall i-CSRMT Framework concepts Classification.....	<b>Error! Bookmark not defined.</b>
Figure 4.13: A meta-model for i-CSRMT at an organisational level.....	84
Figure 5.1: Unified approach model to i-CSRMT.....	58
Figure 5.2: Structure of the Fuzzy Asset Criticality System (FACS).....	97
Figure 5.3: Rules Set for FACS.....	99
Figure 5.4: Sample of Rules.....	100
Figure 5.5: Classification process about the primary analysis and methods that have been used to build the experiment.....	106
Figure 6.1: Architecture of i-CSRMT.....	116
Figure 6.2: Features and components of i-CSRMT.....	117
Figure 6.3: Super Administrator Dashboard.....	<b>Error! Bookmark not defined.</b>
Figure 6.4: Super Admin Login.....	119
Figure 6.5: Super Admin Manages Company.....	120
Figure 6.6: Admin Authentication form.....	120
Figure 6.7: Company Admin Homepage.....	121
Figure 6.8: Add Company details.....	122
Figure 6.9: Actors and Role.....	123
Figure 6.10: Adding and Managing Actors Roles.....	123

Figure 6.11: Actors Roles and Permissions .....	124
Figure 6.12: Managing Projects .....	125
Figure 6.13: Managing Asset Inventory .....	126
Figure 6.14: Threat Modelling .....	127
Figure 6.15: Risk Assessment .....	128
Figure 6.16: Risk Impact Rating .....	128
Figure 6.17: Implement control measures.....	129
Figure 6.18: Evaluate control effectiveness .....	130
Figure 7.1: Evaluation Approach for the Proposed Framework .....	131
Figure 7.2: Roles of Actors and permission.....	146
Figure 7.3: Set Actors permission.....	147
Figure 7.4: Asset criticality Result.....	151
Figure 7.5: Asset criticality graphical chart .....	152
Figure 7.6: Threat and vulnerability profile.....	155
Figure 7.8: Performance of the features on each of the classifiers for predicting risk types .....	158
Figure 7.9: The accuracy of different classifiers for various types of input binary features.....	160
Figure 7.10: The accuracy of different classifiers for various types of features transformed by applying PCA.....	160
Figure 7.11: Precision result performance measure for KNN classifier for the various risk types based on the different features .....	<b>Error! Bookmark not defined.</b>
Figure 7.12: Recall result performance measure for KNN classifier for the various risk types based on the different features .....	<b>Error! Bookmark not defined.</b>
Figure 7.13: F1 result performance measure for KNN classifier for the various risk types based on the	
Figure 7.14: Risk likelihood .....	162
Figure 7.15: Risk Impact factor selection .....	163
Figure 7.16: Calculated Risk Level.....	164
Figure 7.17: Control Effectiveness Result .....	166
Figure 7.18: Control measure implementation .....	167
Figure 7.19: Risk Assessment overview .....	168
Figure 7.20: Acceptability ratings of the CSRM Framework using six different evaluation criteria .....	<b>Error! Bookmark not defined.</b>

## PUBLICATIONS BY THE AUTHOR

Date of Publication/Reference	Title	Journal
(H. Kure and Islam, 2019)	<b>Kure, H. and Islam, S., 2019. Cyber Threat Intelligence for Improving Cybersecurity and Risk Management in Critical Infrastructure. <i>Journal of Universal Computer Science</i>, 25(11), pp.1478-1502.</b>	<b>Journal of Universal Computer Science: J.UCS special issue on Cyber-attack Detection and Response</b>
(H. I. Kure and Islam, 2019)	<b>Kure, H.I. and Islam, S., 2019. Assets focus risk management framework for critical infrastructure cybersecurity risk management. <i>IET Cyber-Physical Systems: Theory &amp; Applications</i>, 4(4), pp.332-340.</b>	<b><i>IET Cyber-Physical Systems: Theory &amp; Applications</i>,</b>
(Kure, Islam and Razzaque, 2018)	<b>Kure, H.I., Islam, S. and Razzaque, M.A., 2018. An integrated cyber security risk management approach for a cyber-physical system. <i>Applied Sciences</i>, 8(6), p.898.</b>	<b>The impact factor of Journal of Applied Sciences 1.69, Special Issues on “Security and Privacy for Cyber-Physical Systems”, 2018.</b>
2021 (Under Review)	<b>Critical Infrastructure Cyber Security Risk Management Using Machine Learning Approach</b>	<b>Neural Computing and Applications (Impact Factor 4.774)</b>

### List of Abbreviations

<b>Abbreviation</b>	<b>Description</b>
i-CSRМ	Integrated Cyber Security Risk Management
CPS	Cyber-Physical Systems
ML	Machine Learning
DisCos	Distribution Companies
i-CSRMT	Interested Cyber Security Risk Management Tool
TTP	Tactics, Techniques and Procedures
IOC	Indicator of Compromise
CTI	Cyber Threat Intelligence

## CHAPTER ONE

### 1. Introduction

The primary objective of CPS is resilience by delivering its users an uninterrupted services based on relying on the most valuable assets such as information and communication networks, and digital data for its continuous reliable service (Almoghathawi, González and Barker, 2021). These assets necessitate the attainment of reliability, stability, and performance, all of which necessarily requires the tight integration of technological control systems, computing and communication (Kim and Kumar, 2013). However, the cyber-physical systems (CPS) complexity and the interdependencies among its various components (people, processes, technology, multiple distributed and independently operating systems) has made it an excellent target for cybercriminals. Such systems face different security threats, including system failures (e.g., device failure, system overload), human errors (e.g., lack of access control, medical system configuration error), supply chain failures (e.g., network provider failure, power outage) and malicious actions (e.g., malware, hijacking, cyber espionage (Jalali and Kaiser, 2018). Cyber-security threats lead to any potential risks, and risks can affect all aspects of critical infrastructure. The probability of loss (Dalziell and McManus, 2004) or an uncertain occurrence that may occur and affect the organisation's accomplishment of strategic, operational, and financial objectives are referred to as risk (Jasmin Harvey and Service, 2007).

The significance of protecting the critical infrastructure is important since it can strongly affect the international market economy and the trust foundations between people and societies. Now, more than ever, shielding and securing critical infrastructures is essential, especially in the healthcare sector. The COVID19 pandemic has stressed the healthcare sector's requirements since malicious entities aggressively exploit this emergency for their benefit. For example, there is a considerable number of registered domains on the Internet that contain terms related to keywords, such as "corona", "covid", "covid19". While many of them are legitimate and focus on the pandemic, numerous domains are used to spread malware via phishing and spam campaigns. Therefore, the presence of any successful cyber-attack on the systems causes a devastating effect on the organisation's critical infrastructure, its business processes, and availability of its services, reputation and the economy at large.

On the other hand, the cyber-threat landscape is evolving rapidly because threat actors' motivation and goal, attack pattern, "tactics, techniques and procedure (TTP)", tools to breach systems are becoming increasingly sophisticated. This affects the understanding of risk, its severity, and cascading risk impact level, making risk management challenging for critical infrastructure systems (Fossi et al., 2011). According to a recent Experian report, almost half of all business organisations experience at least one security incident each year (Levin, 2021). That is why global cybersecurity spending is continuously rising to 96 billion US dollars in 2018 (Huyghue, 2021). Despite efforts to develop and defend secure systems, large organisations, particularly critical infrastructure, believe their

infrastructure is vulnerable. The successful execution of effective cyber-attack is growing with higher frequency and on a larger scale. Rather than worrying whether they would be targets of cyber-attacks, IT managers need to understand when a cyber-attack occurs and the consequences. Since cyber-attacks might be inevitable, the problem of risk prediction becomes critical: identifying which areas of a given infrastructure are the most vulnerable allows for preventive action, focusing on effective controls, and assessing the cascading risk effect is fundamental. Therefore, there is indeed a pressing need to gather Cyber Threat Intelligence (CTI) information such as; information about the threats likely to affect the organisation's assets which include; the threat actor's behaviour, used TTP and other relevant properties so that risk type can be predicted. Researchers' detailed research on different aspects of the cyber-attack problem focuses primarily on these three topics: prevention, detection, and analysis.

However, only a few works proposed prediction models, such as; (Parhizkar, Rafieipour and Parhizkar, 2021), (Kure *et al.*, 2021), (Xiong *et al.*, 2021), which allowed for the adoption of preventive actions to avoid disruption services. These papers examined the demographics of users' (Hanus, Wu and Parrish, 2021), network connectivity behaviour (Aakaash *et al.*, 2021), and web browsing behaviour (Yavneh, Lothan and Yamin, 2021), website features (Alqahtani *et al.*, 2020), network mismanagement details (Albladi and Weir, 2020) and historical incident reports of organisations (Veeramachaneni *et al.*, 2016) to predict cyber incidents. Despite these contributions, no work has focused on integrating ML for predicting risk types within a risk management process.

Additionally, there is a lack of focus on determining asset criticality and evaluating the effectiveness of existing controls to improve the overall risk management process. This research shows that many critical infrastructures tend to retain cyber-security countermeasures and techniques which have been proved inadequate in the past, and at the same time, they resist adapting more efficiently and new technologies. In summary, critical infrastructures need a comprehensive risk management approach that ensures that their critical assets are adequately secured, threats are correctly predicted, and controls are successfully evaluated and implemented. This research contributes to addressing these limitations by proposing a practical i-CSRSM framework for critical infrastructure.

## **1.2. Statement of the Problem**

Academia, researchers and industry experts have given various descriptions, views and challenges of critical infrastructure on cybersecurity issues and challenges (De Bruijne and Van Eeten, 2007). Studies on identifying critical assets, potential vulnerabilities, likely threat impacts, threat identification, and risk management have been proposed in the literature, but they have not been addressed extensively. The cornerstone of a secure critical infrastructure is effective risk management (Adar and Wuchner, 2005), identifying critical assets, assessing vulnerabilities, and evaluating the effects on assets, considering the likelihood of risks is essential. However, the main challenges in

existing risk management approaches are due to increased systems complexity, the evolution of the risk level, the rapid development of the cyber-attack landscape and affecting the understanding of risk and its severity, human-factor threats that include unintentional security breaches, lack of employee awareness and finally lack of CTI adoption. Other challenges include the lack of focus on cascading failures interdependency of critical infrastructure components. These problems and several others have limited the goal of critical infrastructure to evaluate future risks continuously and to prioritise controls at all levels. In order to develop a solution, identified problems from the perspective of this research include:

- **Need for a comprehensive CSRM process model for critical infrastructure:** The need for a comprehensive process that incorporates systematic activities for the implementation of CSRM in critical infrastructures is required. Comprehensive risk management is a continuous, dynamic and organised approach that helps understand, manage, and communicate risk for an organisation's benefit. CPS components are interconnected, and security threats are growing. Therefore, a comprehensive risk management framework that provides a holistic overview must help look at several components simultaneously. The success of the risk assessment relies on the unique features of each component of the infrastructure.
- **Changes in risk level and the lack of new techniques like machine learning for a particular risk type prediction:** There are difficulties in an accurate prediction of risk type, risk level calculation and severity, allowing organisations to prioritise and manage the risk of evolving cyber-attack landscape. Proper CSRM for critical infrastructure is an on-going activity that enables and facilitates the control and management of organisations' threats. Every existing risk cannot be prevented; however, preceding knowledge allows the organisation to make informed decisions. Therefore, new techniques like machine learning to detect threat patterns and accurately measure risk type and level are needed to improve CSRM activities in critical infrastructure. The input features from the CSRM concepts such as threat actor type, location, motivation, skill, intended goal, and resource availability, control types, "tactics, techniques and pro)," and the asset types are extracted from the available datasets and used into machine learning classifiers for predicting the risk type before calculating the risk level. It is thereby speeding up the initial risk identification and classification phases in a risk management process. This approach helps organisations plan their incident response functions adequately and take preventive security threat measures in advance.
- **The need to adopt CTI for improving the overall CSRM:** CSRM for critical infrastructure is challenging due to the constant changes in a threat actors attack pattern, motivation and intention. With this challenge of cyber exploitation and malicious activity becoming increasingly sophisticated, threat actors, TTP constantly evolving and impacting individuals and organisations' daily activities, it is critical and urgent to gather information about the threats likely to affect their

organisation. Existing risk management approaches have not considered the necessity of adopting concepts from CTI and other theories for improving CSRM in critical infrastructure. Therefore, organisations should adopt CTI for improving CSRM to detect and respond to both known and unknown threats and support determining the proper risk level. Integrating CTI to support CSRM helps in dealing with the evolving threat actor profile and attack trends, and the organisation can make the strategic, tactical and operational decision for improving overall cybersecurity.

- **Lack of focus on cascading effects of cyber-security risk in critical infrastructure organisations:** Assessing and mitigating cascading effects across critical infrastructure is one of the most complex problems in critical infrastructure protection. Cascading impact is caused by physical, technological, human or natural disaster failure generating a sequence of other events in the system and disrupting services. The initial vulnerability or impact can trigger other occurrences that lead to significant consequences; this occurs when critical infrastructure components are interdependent.
- **Tool that supports the practical Risk Management activities are required:** The overall risk management approach involves some complexities, especially risk identification and quantification. It requires a reasonable amount of effort for doing the activities under the risks management process. Therefore, this research presents i-CSRMT to support the risk management activities and minimise the efforts required to perform the risk management activities and provide accurate information about the risks. The i-CSRMT can be simultaneously accessed and used by multiple users and allows managing numerous different projects simultaneously.

### 1.3. Research Questions

The research questions were developed in response to the literature review and the potential need to enhance risk management practice. The rationale behind this study is developing a systematic framework that supports organisations with critical infrastructure to adopt CTI to improve i-CSRMT that detects and responds to both known and unknown threats and supports the use of ML techniques to determine the proper risk level. Therefore, this research focuses on providing a framework that includes CTI and ML techniques as an integral part of the i-CSRMT process for critical infrastructure organisations. A current literature review is conducted to identify and summarise the following fundamental issues that need to be addressed:

**RQ1:** What are the key theoretical concepts (such as CTI) necessary for improving i-CSRMT for critical infrastructure protection?

**RQ2:** How can organisations systematically implement the i-CSRMT framework?

**RQ3:** How can organisations use Machine learning techniques to predict risk types to support i-CSRMT activities accurately?

In response to the research questions mentioned above, this research develops an i-CSRSM framework that allows for a comprehensive understanding of cybersecurity risk management for critical infrastructure. The framework offers a collection of concepts and a process that are interrelated to enhance the performance of critical assets, their vulnerabilities, threats, and risks in critical infrastructures by providing:

- i. A comprehensive understanding of i-CSRSM and the concepts is needed to achieve the overall protection of critical infrastructure. This is achieved by integrating CTI concepts extensively for improving existing risk management and cybersecurity practice. We consider several concepts relating to CTI such as threat actor, TTP, indicator, and incident and integrate them with CSRSM concepts such as threat, actor, vulnerabilities, assets, controls and risks.
- ii. An implementable process to support critical infrastructures.
- iii. To enable the automation of risk type prediction, we are introducing a machine learning framework. The framework takes data, builds the features, applies machine learning algorithms and gives results.

#### **1.4. Research Aim and Objectives**

This research proposes and develops an i-CSRSM framework for an effective risk management practice within critical infrastructures to improve critical assets protection and resilience. The objectives are listed below:

**RO1:** Develop an i-CSRSM framework that adopts theoretical concepts to improve CSRSM to protect critical infrastructures.

**RO2:** Proposes a process for i-CSRSM activities that can be implemented based on current industry standards, frameworks, and models. The process includes evaluating the effectiveness of existing controls and recommending new control actions in areas where security improvement is needed to protect their systems from potential cyber-security risks and threats. A real-life case study is used to investigate the usability of the proposed framework.

**RO3:** Integration of techniques such as machine learning for risk prediction and accurate information about the risk impact level.

**RO4:** Develop a dedicated integrated cybersecurity risk management tool (i-CSRMT) that automates the overall i-CSRSM process enabling organisations to continuously identify and quantify risks within a reasonable amount of time.

**RO5:** Propose the use of fuzzy logic for the purpose of asset assessment in a critical infrastructure.

#### **1.5. Contribution of the Research**

The research has made significant contributions by developing a comprehensive framework that incorporates various concepts and improves risk management across critical infrastructure. This novel and state of the art framework respond to the research problems and questions. The following are the study's four novel contributions:

- I. **Contribution 1:** The i-CSRSM framework contributes to the existing state of the art literature with its novel approach that comprises of concepts developed by integrating the existing risk management concepts with the STIX model concepts. Furthermore, the frameworks process consists of a systematic collection of activities and steps that expresses the conceptual framework into strategies, plans, and actions that critical infrastructure can use to achieve risk management. The framework further evaluates the effectiveness of existing controls within the process, and this effectively determines suitable risk mitigation actions for controlling the risks. We apply a set of criteria used to compare evidence by following the proposed comprehensive assessment model.
- II. **Contribution 2:** The i-CSRSM framework proposes using machine learning within the i-CSRSM activities to predict risk types and improve the overall risk management process. The framework integrates CTI (STIX) with CSRSM concepts such as threat actor, assets, controls and TTP, then applies these features to the different machine learning classifiers and then gives results. In general, the model:
  - For predicting risk type, we explore the suitability of the machine learning algorithms to identify the risk type, thus giving organisations an early warning to plan ahead of the threat actor to prevent a powerful attack from occurring.
  - We carried out an extensive experimental evaluation of seven (LR, RF, NB-Multi, NB, DT, NN and KNN) machine learning algorithms to evaluate each algorithm's effectiveness.
  - Displays the best algorithm with a higher accuracy value in predicting risk type.
- III. **Contribution 3:** The development of an integrated i-CSRSM tool (i-CSRMT) to help risk management activities is the thesis' third contribution. The tool's objective is to minimise the efforts required to perform the risk management activities and provide accurate information about the risks to implement the appropriate controls. It provides a comprehensive workflow to guide the organisation through individual activities, starting with defining the organisational context and applying risk controls. Moreover, it also integrates methods for risk calculation to reveal hazardous threats. Therefore the tool aims for an effective risk management practice within critical infrastructure. Furthermore, this research evaluates the proposed frameworks applicability on a real-life case study to solve existing problems. The evaluation result indicates that the proposed i-CSRSM framework can sufficiently support organisations to be more risk-informed and address risks within the organisation's significant complexity. Integrating machine

learning with the i-CSR framework allows faster detection of threats, alerting of risk, and providing appropriate controls in managing overall risks. It also supports making practical suggestions for the improvement of the i-CSR framework.

## **1.6. Empirical Evaluation**

The significant contributions of this research are evaluated using empirical methods. Firstly, to determine the framework's usefulness; a case study approach is combined with action research. Combining action research and case study enables the framework to be implemented in real-life contexts. This includes; collecting data through the participation and collaboration of stakeholders within the study contexts. A case study is an in-depth study investigating real-life context challenges (Benbasat, Goldstein and Mead, 1987). The three main reasons for using a case study in the world of information management (Walsham, 1995) are to; 1; enable a researcher better to understand an information system in its natural setting and generate conclusions from practice, 2; supports a researcher to answer the "how" and "why" questions for establishing clear findings, and 3; enable the researcher to study the complexity of a process that is being followed. Therefore, this research employed a case study to implement our proposed framework, collecting feedback regarding the study's validity and areas that require improvement. The third chapter provides a comprehensive overview of the research methodology, design, and evaluation used in this research.

## **1.7. Outline of the Thesis**

The first chapter discusses the background and motivation for this study and the critical research questions. The rest of this thesis is structured as follows:

**Chapter Two:** This chapter discusses the relevant literature relating to risk management practices for critical infrastructure, background knowledge, discussion, identification of existing gaps and the motivation of the i-CSR framework.

**Chapter Three:** This chapter outlines the research methodology used to address the research objectives and validate the proposed framework's applicability.

**Chapter Four:** The main contribution of this research is presented in this chapter. It presents the proposed framework development, which includes a conceptual model upon which this research is based. This chapter supports a better understanding and identifying the fundamental concepts of the research area for this thesis. By developing research questions and research objectives, identifying ideas is easier because it determines what information is needed and how it relates to the research area's scope.

**Chapter Five:** Another vital contribution of this research is process development. This chapter outlines the proposed framework's approach, as well as systemic activities and steps. Organisations

who wants to implement the framework and understand their cybersecurity status can adopt these activities and steps.

**Chapter Six:** This chapter describes and outlines the i-CSRMT tool's architectural layout, functionality and specifications, and a description of the tool.

**Chapter Seven:** This chapter presents the evaluation of the i-CSRMT framework. The various approaches adopted for validating the research are presented in this chapter. The validation process delivers the methods and procedures used to acquire the necessary information to assess the proposed framework's ability to satisfy the research aim and questions.

**Chapter Eight:** This chapter discusses the i-CSRMT framework compared to other literature works and presents the basis for identifying the framework's applicability and necessary improvement.

**Chapter Nine:** The conclusion chapter highlights the significant contributions of this thesis and future research direction.

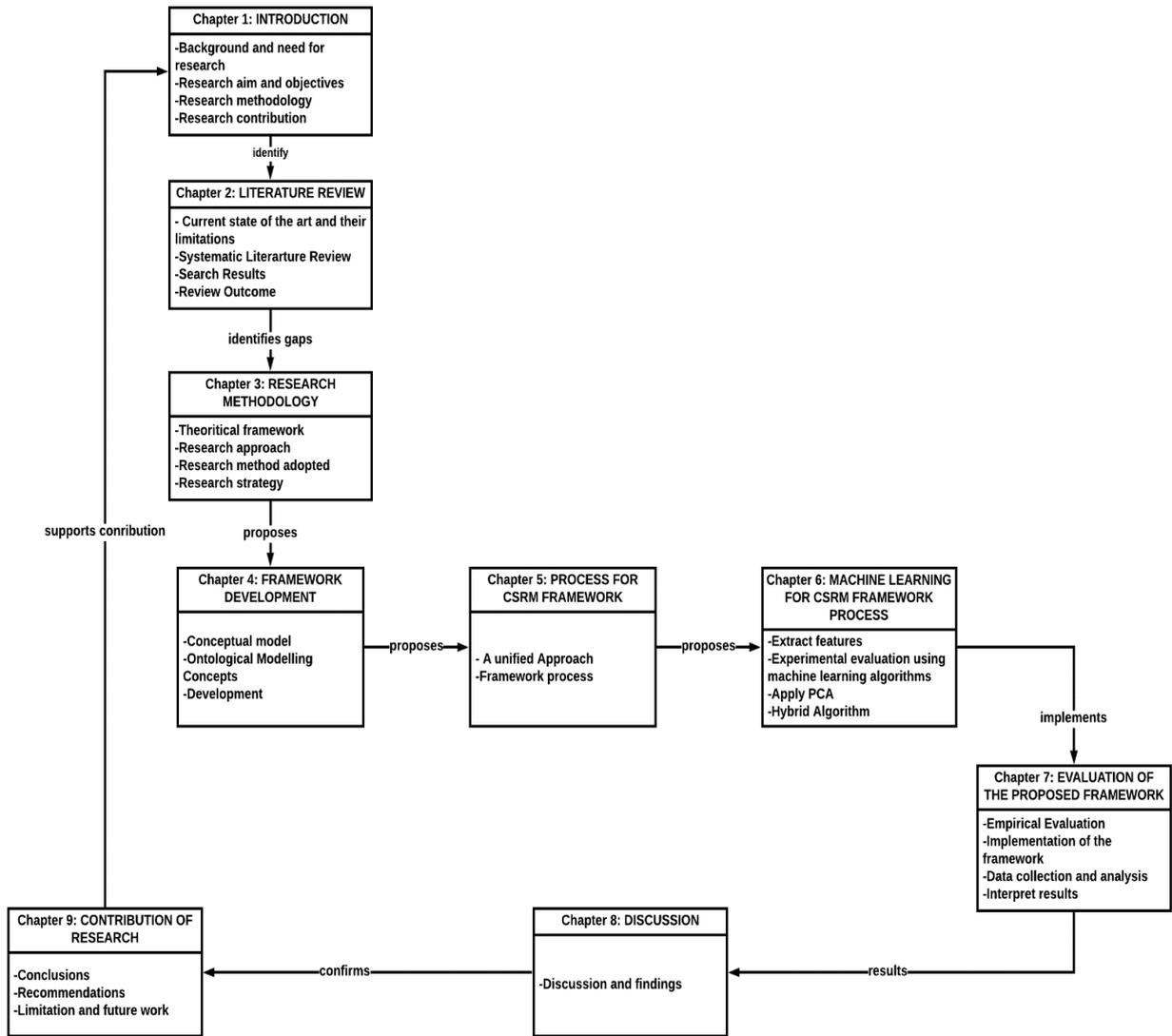


Figure 1.1: Thesis Structure

## 1.8. Chapter Summary

This chapter presents the thesis's research framework, describes the problem domain that needs to be addressed, and the current measures utilised to tackle the challenges and how it aims to overcome those issues. The chapter also included a list of important research questions that would be addressed throughout the thesis. The research's contributions to answering the research questions are also discussed, and the chapter concludes with a summary of the whole thesis.

## CHAPTER TWO

### Background and Literature Review

#### 2.1. Introduction

A common understanding of the research area's critical aspects, including an outline of risk management is essential for the research background. The researchers addressed the primary security concerns in risk management and the types of controls for dealing with these issues. The chapter also discusses relevant works that follow a similar approach to the one included in this work. As a result, the first section of the chapter provides the context for risk management. The second section includes related works in cybersecurity, risk management in CPS, risk predictions leveraging machine learning algorithms, risk management frameworks/standards/guidelines and case study, techniques for risk assessment, many of which are similar to the methodology suggested in this report. Also, the study of related works provides a summary of the limitations of each methodology. The literature review lets the reader consider existing challenges, potential strategies, and the limitations of the present state of risk management.

It is essential to provide a common understanding of the research area's crucial aspects, including an overview of risk management. The chapter presented the primary security issues in risk management and controls for addressing these issues. The chapter also presents related works that are similar to the approach pursued in this work. Hence, the first part of the chapter provides the background of risk management. The second part consists of related works in the area of cybersecurity, risk management in CPS, risk predictions using machine learning techniques, risk management frameworks/standards/guidelines, case studies and cascading impact/effects techniques for risk assessment, all of which have similarities with the approach proposed in this research. Also, the review of related works includes a narration of the limitations associated with each technique. The literature study gives the reader an understanding of existing problems, proposed solutions and weaknesses of the current state of the art in risk management.

#### 2.1. Overview of Critical Infrastructure Systems

Traditionally, societies have depended on a broad of services alongside the infrastructures that provide them. Over time, some of these infrastructures have become critical and vital to the community to support life every day. Critical infrastructure has evolved as an essential component in modern societies, especially in handling tasks that are typically dependent on reliable and secure operation. These are socio-technical systems, and they offer services to the community. They are considered relevant for the regular and daily functioning of the community. The critical infrastructures systems are considered assets and systems that can be either physical or virtual so that

different countries depend on these infrastructures for thriving (Ellinas et al., 2015). Monitoring, controlling, and enhancing these infrastructures' security are incredibly critical to avoid disrupting their effectiveness.

These critical infrastructures constitute individual subsystems that escalate life in the community. Destruction or incapacity of the essential infrastructure systems is said to have a debilitating impact on the national economy, security, national health or public safety, or a combination of all these matters. Control and monitoring of critical infrastructures are essential to avoid operational disruption and normal operations due to component faults, attacks or even natural disasters. The US Department of Homeland Security (DHS) presently describes a critical infrastructure as *“systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters”*. “A critical infrastructure at the European Union level specified in a Council Directive defines critical infrastructure as *“an asset, system or part thereof located in the Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member state as a result of the failure to maintain those functions.”*

When critical infrastructure systems are well secured, this can help them resist internal and external disturbances, and they are also able to operate on an acceptable efficiency level even when several disturbances occur. To improve the resilience of critical infrastructure systems, this is the main objective of the stakeholders. Essential systems of infrastructure resilience are considered a practical and sustainable application of critical infrastructures by all the stakeholders to undertake tasks for the citizens, the government, and the economy. The following activities leading to the essential systems of infrastructure resilience have been proposed.

- Preparation of the critical infrastructure systems specification based on the structural analysis- the essential elements and vulnerable points, dependencies and interdependencies are identified.
- Running a dynamic analysis to help in the identification of most critical risk scenarios- generally, the subject of research or simulation is the propagation of the consequential impacts of essential systems of infrastructure phenomena, an identification of the effects of threats, analysis of the common failures, and system response to a loss.
- The most challenging risk scenarios are prioritised, and those taken into account later during risk management.

## 2.2. Critical Infrastructure Domains

There are different categories of critical infrastructure systems. Each of these categories is found to be essential to the development and welfare of society. Without a significant operation and functioning of these segments in the organisation, this can deter the service scope and the government's effectiveness to run the community's day-to-day governance. There are varying accounts of the critical infrastructure classifications, which determines the sort of role that it plays in our lives- with the United States President's Commission on Critical Infrastructure Protection (PCCIP) as a pivot element in categorising critical infrastructural systems (Moteff, Copeland and Fischer, 2003). A PCCIP report, as cited in (Moteff, 2005) proposed eight classifications of essential systems of infrastructure, including;

- **Information and Communications-** handles information flow within every society.
- **Electricity and Power Systems-** the sectors that handle the central generation of lighting across all society parts.
- **Oil and Gas-** this sector dictates the availability of natural resources for energy development that will run other critical industries.
- **Transportation and Storage-** the sector is relevant to the movement of consumable goods that can sustain any nation's feeding situation.
- **Banking and Finance-** the sector is critical to the value of financial stability within any society.
- **Transportation-** This includes all the various systems like the airline, trains, cars waterways that allow for smooth movement of people from one location to another.
- **Water Supply System-** distributes potable water throughout any society.
- **Emergency Service and Government Services-** all quick response lines to emergencies such as the ambulance services, fire fighting service

Various domains and sectors such as the power grid, healthcare, information technology, communication, and food and agriculture have critical variant infrastructures, and they may find a top-down risk assessment framework to be essential to their effectiveness (Committee, 2010). Risk management is a routine in most organisations. Many organisations avoid cyber-attacks, financial loss, fraud or a failure to meet production expectations by implementing risk management strategies to prevent such events. A successful organisation relies on many factors; the influence of these factors varies from domain to domain. Therefore, this section describes the critical infrastructure of various domains, their limitations, security challenges and characteristics. The information gathered for each critical infrastructure domain is needed for the successful risk management process as well as the threat modelling activity in chapter five

### **2.2.1. Healthcare Infrastructure**

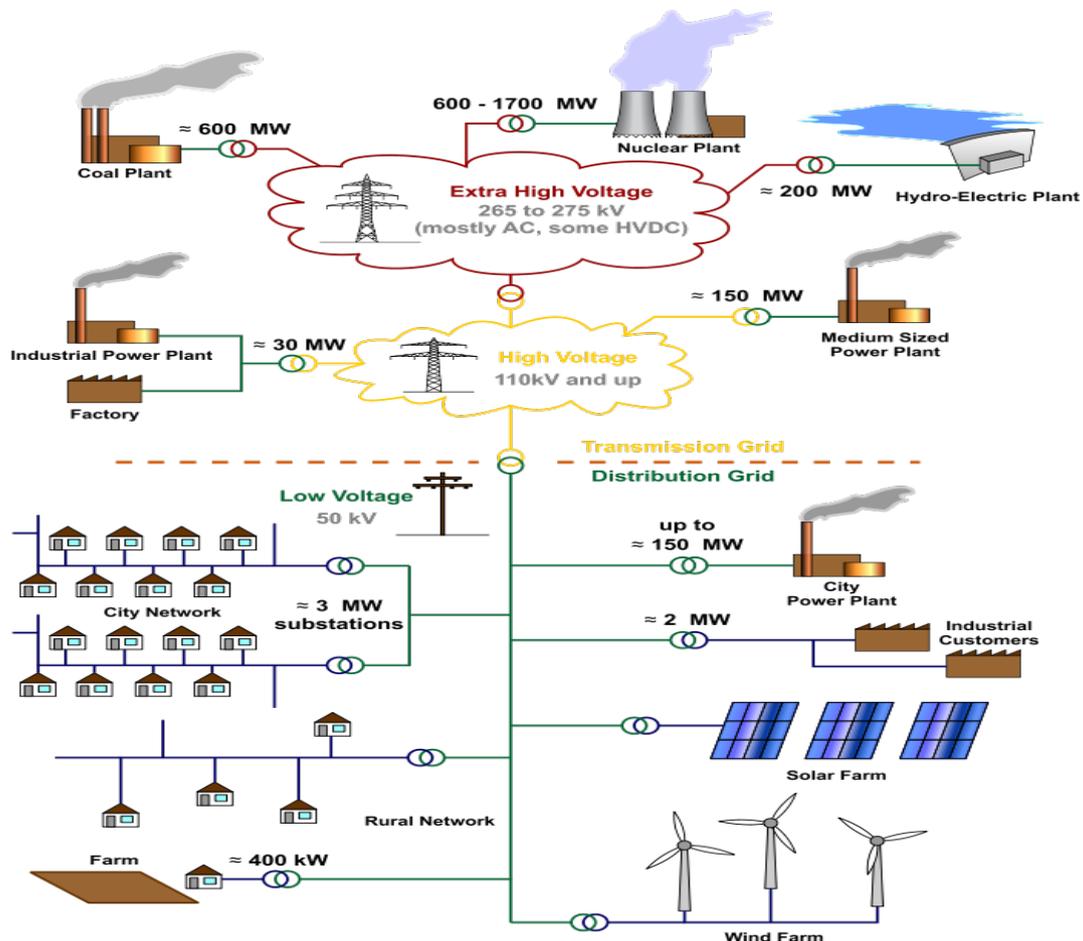
A risk management platform's success in the health care system depends on creating and maintaining safe care systems to reduce opposing events and improve human performance (Organization and Control, 2008). However, healthcare systems, like other critical infrastructure domain, face threat-related issues. These issues include; malicious actions (hijacking, cyber espionage, malware), system failures (device failure, system overload), human errors (misidentification, medication errors, medical system configuration error, lack of access control), supply chain failures (power outage, network provider failure) (Argaw *et al.*, 2020). Protecting healthcare systems is essential because it affects the international market economy as well as peoples trust. Looking at the recent COVID 19 pandemic situation, the healthcare systems has become a target for threat actors by exploiting the systems for their selfish interest.

Effective risk management at every level of the health service can reduce potential risks. Risk management in the health care system is explicitly concerned with improving the quality and safety of healthcare services with the help of risk management processes to identify the circumstances and opportunities that may put patients at risk of harm and then act to prevent or control those risks. Risk management has become an integral part of the healthcare administration. Therefore, serious consideration to implementing and supporting risk management programs to protect their assets and minimise financial losses is recommended (Singh and Ghatala, 2012).

### **2.2.2. Power Grid Infrastructure**

This section offers a high-level description of the power grid structure. As seen in Figure 2.1, the infrastructure comprises three major components: a power plant, a transmission substation, and a distribution grid. The power grid is a network of power lines and related infrastructure that transmits and distributes energy around a geographical region. Transportation, distribution networks, sanitation, power, and public services such as colleges, clinics, post offices, and even prisons are examples of such facilities (Moteff and Parfomak, 2004). The electric sector's cyber-physical systems include industrial control systems (ICS), which enable digital control of machinery's physical operations. Whereas generation machinery such as turbines was once only manually regulated, equipment is now primarily protected and managed by ICS synchronously, by automation, and sometimes remotely. Because of technical advances, most power grids are becoming highly susceptible to cyber-attacks. Modernization activities of older grid system elements to integrate new digital automation, or smart grid innovations, have culminated in a more significant number of Internet protocol (IP) powered grid network access points (Yan *et al.*, 2012). The convergence of information technology (IT) and operational technology (OT) in ICS broadens the cyber vulnerability environment by adding new threat vectors due to improved device communication. Networks may become less reliable when constantly reconfigured to provide one-time access for a particular purpose or ease and are never fully

restored. Remotely available infrastructure is much more prone to public discovery via unsecured networks or the Internet. According to (Amin, 2011), each structure of the US power grid (generation, transmission, and distribution) presents analogous and distinct risks to the reliable delivery of electricity through cyber-physical properties.



**Figure 2.1:** An overview of the Power Grid System

### 2.2.3. Transport Infrastructure

The transport infrastructure also faces some security challenges that could negatively impact its operations like the other critical infrastructure domain. Some of the challenges faced by the transport binding infrastructure domain are:

- The effectiveness of the existing controls is not being continuously checked and adequately. Existing controls need to be checked continuously, recorded and observed to identify those controls that are not meeting the requirement and additional controls that need to be implemented.
- Lack of cybersecurity information sharing amongst the critical infrastructure domains.

- Most transportation networks come with many legacy systems that pose a severe security threat to the organisation's functionality beneath, mainly due to obsolete security controls and mechanisms that initially aimed to prevent product theft and tampering. Over the last few years, however, the transport critical infrastructure shift to an interconnected version of themselves, making unnecessary and potentially dangerous such systems' co-existence.

#### **2.2.4. Financial Infrastructure**

Financial misadventures in financial and non-financial companies and government institutions are creating financial crises, demonstrating the need for risk management in different ways. In most regulatory agencies, poor risk control is a vital issue. By identifying key risks, obtaining consistency, understandability, operational risk measures, choosing the risks to reduce and which to increase and by what means, and establishing procedures to monitor the resulting risk position, risk management is the process by which managers satisfy; reliable risk measures, estimate the size of potential losses, and mechanisms to monitor risks (Pyle, 1999). In the banking industry, risk control helps manage liquidity, credit, business, operational, and foreign exchange threats (Županović, 2014). Risk management is the method of safeguarding investments and reducing financial loss for a company. Risk management includes practices to reduce the incidence and intensity of unpredictable events, mitigate harm, and foster a high-reliability performance framework (Singh and Ghatala, 2012).

#### **2.2.5. Telecommunication Networks**

Unauthorized individuals may gain access to private information and critical infrastructure through computer networks, satellite communication systems, and connections. One of the critical networking infrastructures that pose significant security threats is satellite networks. Attacks on networks, such as DoS (Distributed Denial of Service), may make corporate and military communications inaccessible at crucial periods, stopping legal clients from accessing essential resources (Abouzakhar, 2013).

#### **2.2.6. Software Development Projects**

Software development is a knowledge activity that requires a wide range of technical advances and necessitates a high degree of expertise. Because of these and other reasons, the amount of danger involved with each project operation is vital to a project's performance. It is not enough to be mindful of the threats as a project manager. There are aspects of complexity in undertaking a good software development project. This is what is referred to as a project chance. Project leadership must recognise, evaluate, prioritise, and address all significant risks for a software development project to succeed. Choosing a software development approach and related activities is a significant and inherently dangerous choice for a software development team (Selby, 2007). Increased consumer loyalty, reduced failure rates, quicker production cycles, and a response to quickly evolving specifications are all commitments offered by agile processes. Agile processes are iterative.

Systems Development (SD) projects are carried out by many organisations yearly. Software development activities require extensive resources such as time, personnel, and money with complex inter-organisational development processes and sophisticated technical requirements (Warkentin *et al.*, 2009). Businesses rely on software growth. In most cases, software projects have been carried out in an unpredictable environment that is likely to have drawbacks that harm a business's successful result. Evaluation of projects that have been carried out has revealed that most projects that did not succeed were already expected to fail. A successful project is only successful if it meets functionality, reliability, maintainability, portability, efficiency, integration and operability and delivered on time and within the expected budget. Just a few projects are completed on-time and within budget, but most of the projects are either cancelled or changed. The high failure in managing risk when developing a software project is due to managers not taking suitable measures to assess and manage the risk involved in software projects (Addison and Vallabh, 2002).

### **2.3. Critical Infrastructure Interdependency**

Critical infrastructure systems have three primary levels that are constituted in a vertical classification. These are the system level, the sector level, and the element level. The system level is considered the basic level, given its functions. It comprises of the socio-economic infrastructure and the technical infrastructure. The technical infrastructure encompasses the sectors that produce and provide specific products such as water supply and energy or technical services such as transport (Elmaghraby and Losavio, 2014). The socio-economic infrastructures are composed of the type of sectors that provide financial or social services. These include healthcare, currency and financial markets, public administration and emergency services. The sector level comprises the subsectors and the individual sectors that are mainly found in critical infrastructure. This level usually presents the classification of distinct sectors together with their mutual links. The transportation sector, for instance, is made up of different subsectors such as energy, water, and inland waterways transport (Elmaghraby and Losavio, 2014). The vital specific elements that form the element level are considered the building blocks of critical infrastructure.

A critical infrastructure system must be considered comprehensively, considering the networked arrangement whereby the individual subsystems are connected through different linkages. Like any other complex system, a critical infrastructure system has various elements with varying levels of importance. Once a risk faces them, a threat or any vulnerability can lead to a situation where the national system is failing. A structural arrangement also leads to creating a broad correlate between the individual subsystems that helps determine the intensity and propagate the impact that critical infrastructures have on society. Failure of critical infrastructures is vital to society as they are the lifeline and the support systems that are called upon to facilitate societal growth and development (Fischer, 2014). Thus, risk management in the critical infrastructure is crucial, and it necessitates

governments to take cybersecurity measures that help to safeguard these essential systems of infrastructure.

### **2.3.1. Interdependency of Critical Infrastructure Domains**

According to (Rinaldi, Peerenboom and Kelly, 2001), four types of interdependencies are recognised for critical infrastructure domains. From the operational perspective, a critical infrastructure domain such as the healthcare domain relies on the correct functioning of other critical infrastructure domain, such as the power grid, telecommunication systems, banking sector and water supply. They may or may not be directly connected to the healthcare system, but they are considered critical infrastructure in the healthcare sector and their correct operation must be guaranteed. Due to the relationships between the infrastructures, each is correlated to the other's state since they are directly correlated. These are typically referred to as interdependencies, and they range from cyber, physical, logical and geographical inter-dependency. The four types of interdependencies include:

- i. **Physical interdependency:** A situation where the operations of one infrastructure depend on the material output of another.
- ii. **Cyber interdependency:** Depending on information conveyed through an information set-up.
- iii. **Geographic interdependency:** When the dependence is basically about the environmental impact that affects several infrastructures simultaneously.
- iv. **Logical interdependency:** When the dependency cannot be categorised as either physical, cyber or geographic.

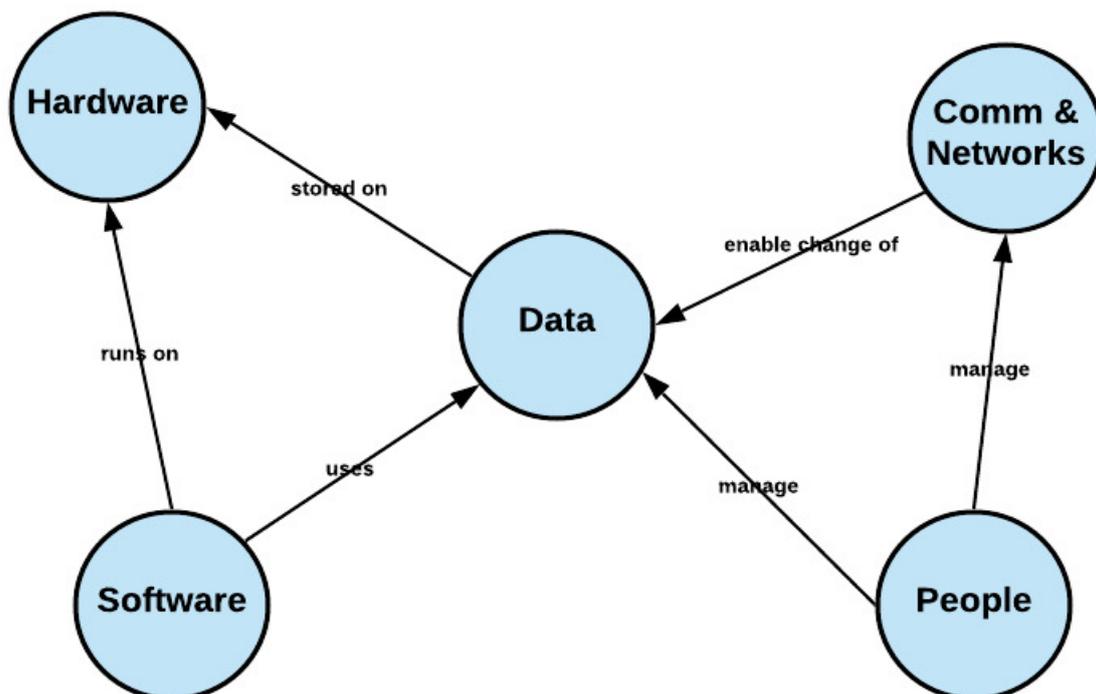
### **2.3.2. Asset Interdependency within a Critical Infrastructure Domain**

Complex ecosystems of interconnected devices in the different domains are presented in this section. From the operational perspectives, critical infrastructure assets rely on the correct functioning of other vital elements. Several standards propose asset taxonomy for important infrastructure sectors such as ENISA (Argaw *et al.*, 2020). For example, databases that store patients' sensitive information in a healthcare critical infrastructure domain, such as personal and contact information, credit card details, examinations' results, prescriptions, and video records from surveillance cameras, are interdependent, as shown in Figure 2.2. Other complex devices that are interconnected and are interdependent include (Mrabet *et al.*, 2020);

- Computers, network printers and scanners
- Firewalls, intrusion detection systems, routers
- Vital signs monitoring systems monitor and analyse most of the patient vital signs while being connected to the corporate network.

- Specialised equipment, such as ultrasounds, X-rays and electrocardiographs, are connected to the corporate network with files stored in databases for each patient.
- IP telephony and telecommunication infrastructure.
- Cloud services
- Industrial control systems (e.g., temperature, access control)

Therefore, investigating how each asset is protected against cyber-attacks is crucial. It is vital to identify and categorise vulnerabilities and threats associated with each asset to secure these assets by examining the attack surface. Some of the consequences that can be presented are loss of personally identifiable information (PII), patient treatment errors and inaccessibility to other patient data. In the healthcare sector, all these consequences can potentially lead to economic effects (e.g., forensic and system recovery service fees), reputation demolition, service inconveniences and, in the worst case, loss of lives (Fournaris, Pocero Fraile and Koufopavlou, 2017). These assets must be secured and protected using authorisation techniques and access control systems.



**Figure 2.2:** Interdependency of Assets

### 2.3.3. Cascading Impact/effect

The cascading impact is an inevitable and often unexpected series of events required to trigger the next case. The study of cascading effects is a central challenge in critical infrastructure security since,

considering the limited risk of specific incidents, they may have catastrophic implications for several critical infrastructures. A cascading impact happens when one infrastructure's failure impacts one or more elements in another infrastructure, allowing the second infrastructure to be partly or wholly inaccessible (Kotzanikolaou, Theoharidou and Gritzalis, 2013). Due to the common-cause failure, each of the concurrently failed infrastructures may lead to multiple cascading chains of their dependent infrastructure failures. As a result, significant effort is required to research cascading effects and examine cascading impact management and defence ((Wang, Zhang and Gan, 2016).

Cascading failure occurs in power grids where one of the components fails entirely or partly, causing the load to be transferred to neighbouring elements in the system. Those surrounding elements are then forced beyond their range, causing them to become overwhelmed and transfer their load to other elements. Cascading failure is a typical effect in high voltage networks in which a single point of failure (SPF) on a completely loaded or slightly overloaded circuit results in a sudden point through all system nodes. This surge current will trigger already overloaded nodes to malfunction, creating additional overloads and bringing the whole device down in a matter of seconds. This failure phase cascades through the system's elements and persists until significantly all of the system's elements are corrupted, and the system is functionally disconnected from its load source. For example, under some circumstances, a broad power grid will fail due to a single transformer's failure.

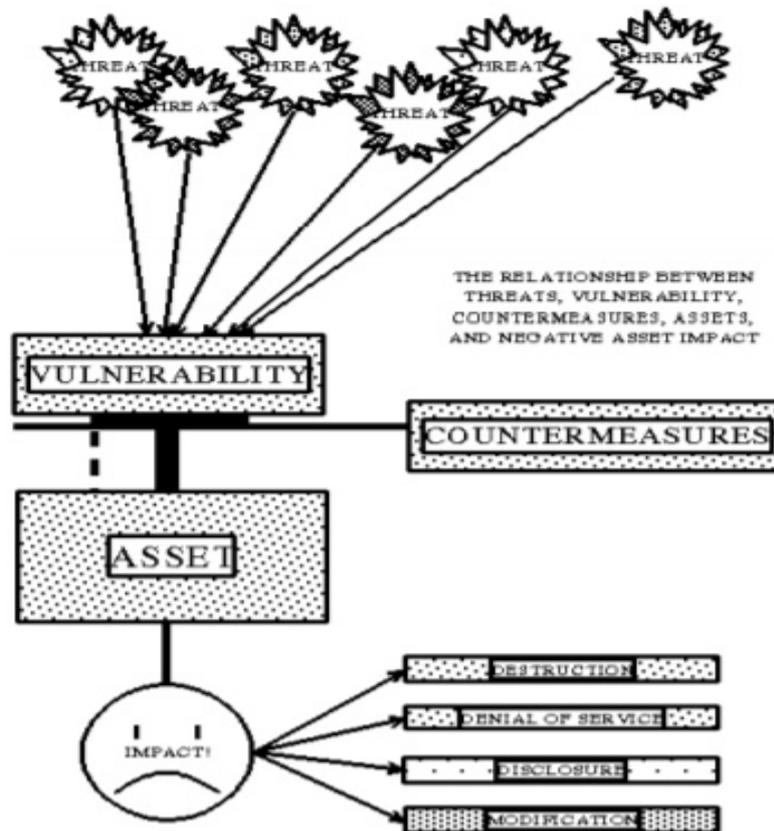
#### **2.4. Risk Assessment Overview**

The risk analysis patterns enable an organisation's management, the information needed to allow sound judgments regarding cybersecurity. Risk analysis procedure indicates the obtainable security controls, computes susceptibilities and appraises the impact of the threats on all vulnerability areas. (Ivanenko, 2020) notes that risks can be considered regarding possibilities and potential consequences with similar definable elements that encompass the settings, assumptions, metrics, and procedures that ensure risk assessments add to a combined indulgence amid critical infrastructure partners. Distinct risk assessment methods help develop an appraisal plan that ends up in proper, scenario-based outcomes and susceptibility calculations, along with assessing the possibility that a suggested threat of hazard will happen. Significant risk analysis terminology includes the following:

- i. Asset- any infrastructure with significance and requires protection.
- ii. Threat- an activity or activity with capability in the future to create damage.
- iii. Vulnerability- a situation of exposed weakness. Where vulnerability is not discussed, there will be no need to develop frameworks for threat activities.
- iv. Countermeasure- Any device or activity aimed at vulnerability reduction.
- v. Expected loss- the imaginably accepted negative effect of assets due to threat execution.

A security risk analysis is the overall consideration of interrelating assets, threats, exposures, and countermeasures to ascertain the current risk level. The degree of risk that remains after looking at all

countermeasures inclusive of vulnerability levels and relative threats is known as residual risk. In practicality, it is the residual risk that has to be accepted or reduced to a point where it can be accepted. When there is a threat within an infrastructure's system, it targets vulnerabilities creating loss where there are no countermeasures to handle attacks. Asset protection is the last goal of risk analysis to reduce threat actions' impacts through residual risk.



**Figure 2.3:** Threat, vulnerability, countermeasures and asset relationship (Jenkins, 1998)

A security risk analysis is an approach used in calculating the risk to computer-related assets and loss attributed to an existing threat. An asset's vulnerability first determines threat analysis by identifying and evaluating the impact of countermeasures set in place. An infrastructure's level of vulnerability to any threat solely depends on the controls/safeguards in place at the time risk analysis has been done (Zografopoulos *et al.*, 2021). Risk analysis assessments are also aligned to initiating an economic balance between the exposure to risk and the consequential impact of these risks. At the core of selecting practical and cost-friendly protective approaches to risk assessments, it is premeditated that the cost of dealing with a specific risk should not exceed the maximum loss associated with the risk. Research by (George and Renjith, 2021) argued that the decision to establish risk assessment measures and countermeasures might be motivated by the critical infrastructure system's relevance.

Thus, risk analysis created for particular assets are demarcated as vital infrastructure, tested and substantiated. This is a process that is indicated in the above linear approach.

#### **2.4.1. Need for Risk Assessment in Critical Infrastructure**

Governments must protect their essential critical infrastructures against natural disasters, terror activities and very recently, cyber-attacks. The management of risks is a shared responsibility among all the stakeholders in the critical infrastructure. These stakeholders include the industry partners, governments, non-government organisations and first responders. According to (Lewis, 2019), the organisations handling high power transmissions need to integrate security to initiate proper disaster preparedness, response and recovery. Accessibility to cyber-attacks on such critical infrastructures in industries like electricity, transportation, and centralised water system services is daily exposed to risk. Such attacks can have detrimental effects, threatening global economies and general lifestyle. The success of critical infrastructure security ideology depends on reliable and meaningful partnerships groomed between government and commercial institutions. Success also depends on the various implementation process and timing (Trigaux *et al.*, 2021). It is essential to identify the risks that could impact critical infrastructure networks' reliability because hackers or terrorist threats are inevitable. The stakeholders also need to consider other vital aspects such as human error, failure of equipment and natural causes. When choosing resolutions that assist in detecting and identifying security risks and malfunctions in systems behaviour, it is necessary to include as many of the risks that stand a chance to affect the infrastructure (Sasaki, 2020).

According to research by (Tweneboah-Koduah and Buchanan, 2018), the modern connected network processes and systems can be a danger to the system control space. This is grounded on the fact that the use of logic-based electrical systems increases risk susceptibility. System protocols such as Control Net, Device Net, Serial Modbus, and Profibus are based on vendor-specific technologies and use different operating systems and internet protocols in overlooking, controlling, and monitoring control operations. The incumbent knowledge of taking measures to safeguard the critical infrastructure has been a critical research interest by different researchers. Research by (Kumar *et al.*, 2021) finds that developing physical boundaries is critical around critical assets. However, among the interconnected critical infrastructures, striking a difference between the 'inside' and the 'outside' is challenging since most infrastructural resources have become technologically interconnected and dependent. This has led to the improvement of the complexity of the system. Research by (Argyroudis *et al.*, 2020) showcases those security risks relative to the critical infrastructure. They argue that there are physical, logical and technological defects in the networking infrastructures that may affect the effectiveness of the critical infrastructures

## **2.4.2. Risk Management methodologies for Critical Infrastructure**

This study's central concept is risk assessment, risk management for critical infrastructure, and machine learning classification to predict risk. These concepts are essential to this thesis's nature and are aligned to completing the primary objectives, characteristics, and functions. Different literature studies define “risk analysis” as a management development to curtail the minutes number of negative surprises from happening inside a system (Lavanya and Malarvizhi, 2008). Since security attempts usually do not ensure total protection against all forms of threats- risk analysis is utilised and expatiated adequately in this thesis. Conducting a risk analysis is crucial as it helps understand where the risks can be identified and make a general consideration of the affected assets. When infrastructure is affected by risks, this creates vulnerabilities that amount to losses. To safeguard infrastructures from risks, this necessitates assets protection and uses a standard framework to guide the implementation of measures and safeguards. Alongside the vulnerabilities, understanding the source of the attacks through risk analysis helps to calculate the risks and the losses and the consequential impact.

(Lewis, 2019) finds that effective risk management on critical infrastructure systems depends on the critical infrastructure community's ability to engage different and shared understanding of risk and integrate a wide range of activities to manage risk. In the United Kingdom, there has been a development of measures and cross-sector risk management plans associated with understanding how risks in critical infrastructure systems should be managed. In different countries, governments make sure that they applaud the responsibility to safeguard the essential systems of infrastructure from terror activities, natural disasters, and in most cases, cyber-attacks (Leita and Dacier, 2012).

### **2.4.1.1. Risk Management Tools**

Risk management tools also play an essential role in increasing risk management processes/activities and decreasing dependence on each particular risk assessment expert's expertise. When working with Critical Infrastructures, specific resources' contribution becomes much more critical and may even be critical for effective Risk Management. A single expert is unlikely to contend with the variety and sophistication of knowledge needed to properly perform a critical infrastructure security risk evaluation (Adar and Wuchner, 2005).

There are different distinct types of tools used for managing risk in all the risk management processes. These tools allow planners to explicitly address uncertainty by identifying and generating metrics, prioritizing, developing responses, tracking risk from components, task or cost. The purpose of the tools is mainly automatically performing the risk management activities; produce the output from the activities. Logically, people like to be creative and create a methodology and tool at a low cost that meets the business needs (Hawk and Kaushiva, 2014). Below is a list of tools used for managing risk:

- **IRAM (Information Risk Analysis Methodology) Tool:** IRAM is designed for business-led information risk analysis methodology. IRAM provides tools to businesses for impact evaluation, threat and vulnerability assessment, and control selection. However, since IRAM is not a web-based automated solution, it does not have resources for continuous tracking and risk report status and workflow to handle unnecessary threats. IRAM is an excellent tool for analyzing risk, but it is not designed to quantify residual risk and cannot independently provide important information on residual risk status because of its centralized and aggregated manner. Therefore IRAM needs to be combined with a tool that can calculate residual risk status and provide strong risk monitoring and reporting capabilities (Creasey and Marvell, 2013)
- **STREAM (Strategies Risk-based Enterprise Assurance Management) Tool:** Acuity risk management provides an attractive, low-cost alternative to spreadsheets for governance, risk and compliance (GRC), scalable from free single-user to Enterprise-wide deployment for the most prominent organisations. STREAM has the advantage in that its framework mappings allow Controls to be mapped to Asset Classes and Threats. Each time an Asset is added to an asset class, STREAM will automatically map all relevant controls and threats to the Asset (Asset is a term used in STREAM to represent a component of the target scope for risk management) (Creasey and Marvell, 2013). However, it does not take any risk predictions.
- **Critical Infrastructure Risk Assessment Support (CIRAS) Approach:** The CIRAS approach aims to create a methodology and tool to help in the selection of Critical Infrastructure protection measures by taking into consideration the effect of traditional CI incidents such as interdependence, cascading, and escalation of the incident. The CIRAS strategy is unusual in that it requires a systematic evaluation of all facets of C.I.s protection policies, including the anticipated risk mitigation and its expense, as well as financial benefits (Bialas, 2016a).

### 2.4.3. Threat Analysis

Threat analysis is the process of moving topics from unknown unknowns to known ones when the risk is fully implicit and alleviated (Chismon and Ruks, 2015). The report considers four different CTI types, including strategic, operational, tactical and technical. (Barnum, 2012) reflects the on-going efforts to generate, advance, and enhance the community-based enlargement of sharing and organizing cyber threat information. (Conti, Dargahi and Dehghantanha, 2018) elucidates the increasing number of cyber-attacks that requires cybersecurity and forensic specialists to detect, analyse and defend against cyber threats in almost real-time. In practice, timely dealing with such a large number of attacks is impossible without intensely perusing the attack features and taking similar intelligent defensive actions; this, in essence, defines cyber threat intelligence notion. (H. Kure and

Islam, 2019) targeted to progress the appreciation of the perception of CTI by awarding a much-needed definition of CTI and producing an idea of the intelligence creation method. (Mavroeidis and Bromander, 2017) introduces the Cyber Threat Intelligence (CTI) model, which enables cyber defenders to explore their threat intelligence capabilities and understand their position against the ever-changing cyber threat landscape. In addition, they used their model to analyze and evaluate several existing taxonomies, sharing standards, and ontologies relevant to cyber threat intelligence. Our results however, show that the cyber security community lacks an ontology covering the complete spectrum of threat intelligence.

In (Mateski *et al.*, 2012) described threat metrics and models for characterising threats consistently and unambiguously. They embedded these metrics within a process and suggested ways in which the metrics and process can be applied and extended. However, a further study regarding how analysts assess threats is needed. In (Sauerwein, Sillaber and Breu, 2018) defined CTI as the obtained unstructured and ad-hoc sources of information that is made publicly available. Therefore, they conducted an in-depth analysis of the unstructured and unapproved use of CTI and investigated its application in organisations. Their analysis revealed that many heterogeneous and overlapping cybersecurity information sources serve as input for information security and risk management processes. However, associated risks and how to extract its value in a compatible way with the organisational requirement are needed. In this paper, (Abu *et al.*, 2018) identifies some challenges relating to CTI, such as threat data being overloaded, quality of threat data that is shared amongst community members, privacy and legal issues which governs the lawful sharing of data and the interoperability issues faced by threat sharing platforms and standards used by the platforms. However, with all these challenges, adopting CTI by organisations to help them minimise future threats still outweighs its lack of adoption.

#### **2.4.4. Threat Taxonomy**

This research investigates the cyber threats and the most targeted assets from the threat actor's perspective. Threat taxonomies respond to the necessity to offer a common language for conveying I.T. threats that could lead to cyber-attacks or cyber-incidents of any nature. The heterogeneous nature of the cyber-security field gave birth to several threat taxonomies from various organisations, where each one of them took into consideration its own specific needs and created a tailored version of threat classification. The majority of the tools mentioned below provide lists and APIs for accessing up-to-date threat details. Some consider these sources to be threat intelligence, but views vary. Serious threat information necessitates a certain degree of (domain- or business-specific) research. This section contains a variety of resources for analysing, generating and modifying Threat Intelligence. Among the critical infrastructure vulnerability sources are:

**2.4.4.1. Frameworks and platforms:** The following frameworks, tools, and services are used for gathering, analysing, generating, and exchanging Threat Intelligence:

- **Collective Intelligence Framework (CIF):** CIF enables you to integrate known malicious vulnerability information from several sources for prevention and mitigation. Vulnerability information includes: Improper Authorization, Authentication Bypass by Spoofing, Improper Input Validation.
- **Cortex:** Cortex enables observables such as IP addresses, email addresses, URLs, domain names, directories, and hashes to be evaluated individually or in bulk mode using a single web interface. The site interface serves as a frontend for multiple analyzers, eliminating the need to integrate this during the study. Analysts may also use the Cortex REST Application Programming Interface (API) to simplify their study aspects.

**2.4.4.2. Formats:** Threat intelligence (mostly Indicators of Compromise (IOCs)) can be shared in standardised formats.

- **Common Attack Pattern Enumeration and Classification (CAPEC):** Analysts, developers, testers, and learners may use CAPEC to strengthen public awareness and protections by utilising a robust vocabulary and classification taxonomy of documented threats. CAPEC's chart includes 541 attack trends and four levels of categorization until February 2021. The taxonomy of CAPEC is based on Mitre's Popular Weakness Enumeration (CWE) (Barnum, 2008) and it provides summaries, attack prerequisites, and solutions for the most common attack trends at any stage of the hierarchy, spanning the entire attack life cycle.
- **The Malware Attribute Enumeration and Characterization (MAEC):** MAEC projects are aimed at creating and providing a standardized language for sharing structured information about malware based upon attributes such as behaviours, artefacts and attack patterns (Kirillov *et al.*, 2011).
- **The Structured Threat Information eXpression (STIX):** The STIX language is a structured way of expressing cyber threat information. The STIX Language aspires to be entirely descriptive, scalable, extensible, and automatable to communicate the full spectrum of possible cyber threat content. STIX allows tool-agnostic areas and offers so-called test frameworks that enable tool-specific elements to be embedded, such as Open IOC (Barnum, 2012).
- **The Trusted Automated eXchange of Indicator Information (TAXII):** The TAXII standard defines a set of resources and message exchanges that, when introduced, enable organisations and product/service boundaries to communicate actionable cyber threat information. TAXII is a collection of principles, protocols, and message exchanges for

exchanging cyber threat knowledge to identify, deter, and mitigate cyber threats (Connolly, Davidson and Schmidt, 2014).

- **The Vocabulary for Event Recording and Incident Sharing (VERIS):** VERIS is a collection of indicators that serve as a shared vocabulary for defining security incidents formally and repeatably. VERIS is a solution to one of the security industry's most pressing and persistent issues: a scarcity of high-quality data. VERIS not only has a centralised format, but it also gathers evidence from the public to investigate attacks through the Verizon Data Breach Investigations Report, which is published publicly at [VCDB.org](http://VCDB.org) (Burger *et al.*, 2014).
- **Web Application Consortium (WASC):** Representatives of the Web Application Consortium established the WASC Threat Classification (Alhanahnah, Jhumka and Alouneh, 2016) to explain and coordinate the challenges to a web site's security. This classification describes the types of attacks and flaws that may contribute to a website, its files, or its users being hacked.

**2.4.4.3. Standards:** Below are links to a variety of Threat Intelligence reading materials, including (scientific) studies and whitepapers:

- **Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK):** ATT&CK is a model and structure for defining an adversary's behaviour when operating inside an enterprise network (Tactic, 2017). ATT&CK is a rapidly growing complete overview for post-access procedures that raises the visibility of the types of behaviour used after a network attack. MITRE is working hard to integrate with other similar constructs, including CAPEC, STIX, and MAEC.
- **The European Union Agency for Network and Security Information (ENISA):** ENISA published its initial version of Threat Taxonomy to aid information collection and understanding of threats related to information and communication technology assets. Some of these threats are related to cyberspace, while others are materialized in the physical-world but affect information and cyber-assets. However, it is worth noting that the taxonomy is maintained chiefly for cyber threats (Marinos, 2016).
- **Common Weakness Enumeration (CWE):** CWE is used for communicating the impacts of vulnerabilities. CTI seeks to understand and characterise vulnerabilities, misconfigurations or weaknesses that are likely to be targeted. It introduces a common weakness scoring system (CWSS), which provides a mechanism for prioritising software weaknesses consistently, flexibly, and openly. It is a standardised approach for characterising weaknesses, thereby allowing organisations to make more informed decisions during the risk management phase and give higher risks (Martin, 2007).
- **Open web application security project (OWASP):** OWASP is an open community dedicated to enabling organisations to conceive, develop, acquire, operate, and maintain

applications that can be trusted. It provides basic techniques to protect against web application security challenges. To ensure consistency and relevance of risks and their impact, we adopted the OWASP risk methodology (Tymchuk, Iepik and Sivyakov, 2017). This methodology helps organisations to estimate risk from business and technical perspectives. Many aspects that contribute to the likelihood and impact of each risk are considered, and therefore the risk's severity is determined.

## **2.5. Related works**

Similar works in security risk management approach for CPS, cybersecurity in smart grid, and security risk management frameworks/standards/guidelines are discussed in this section. A literature analysis in these fields allows the reader to understand the limitations of the current state of the art and understand the complexities of cybersecurity in critical infrastructure and customize this research's foundation.

### **2.5.1. Risk Management in Critical Infrastructure**

Authors in (Yoneda *et al.*, 2015) showcased the existence of critical significance of CPS from a user perspective in an enterprise. First, the office was regarded as a CPS whereby physical security and information security are connected. The CPS risk assessment was performed with a risk assessment approach, and the risk factors in the CPS accounted for using the Risk Breakdown Structure (RBS). With the help of a risk matrix, the countermeasures were proposed and classified and the risk values included in an information security management system (ISMS) for an in-depth risk assessment. The quantitative evaluation helped to show that the prospected solutions could assist in minimizing risk to some extent. (Patel, Graham and Ralston, 2008) proposed a new approach to assess the vulnerability of an organization to breaches in information security. A threat-impact index alongside a cyber-vulnerability index related to the vulnerability trees was presented as a threat-impact index measure. Using these approaches, managers can determine the current state of security, which could help them select optimal security mechanisms. Nonetheless, the probability included in each damage category would be significant in helping the risk managers to be able to quantify the number of risks that are related to the information system. (Hahn *et al.*, 2013) offers a generalized observation of the processes of integrating smart grid security. This includes the set of communication, controls and the physical system components necessary to provide an accurate cyber-physical environment. (Cárdenas *et al.*, 2011) proposed an approach to help detect risks and computer attacks that alter the targeted control systems' behaviour by understanding the implications of the threats and risks to assist in designing a new-attack detection algorithm alongside an attack-resilient algorithm.(Ericsson, 2010)considers the existence of the cyber-security issues, information security domain, together with the concept of the access points in a rather substantiated way in a power system communication (PSC).

(Wu, Kang and Li, 2015) proposed using a quantitative risk assessment approach that centres on the CPS running conditions and helps in a real-time calculation of risks. Using this model, it becomes easier for users to respond to different risks on time, help select and implement comprehensive security measures in helping managers avoid threats and damages that might result. It also helps the users by providing them with attack details such as the type of attack, the frequency, host ID and the target source ID. Nonetheless, a risk assessment approach using this approach requires the inclusion of an automatic identification alongside quantitative analysis methods to help in dealing with several information updates concerning the assets, threats, and vulnerabilities within the CPS. This notion is the research by (Cherdantseva *et al.*, 2016) which examined some of the risk assessment approach based on the factors such as objectives, application domain, risk management stages, impact measurement, and tools. The research also shows the need for improvement regardless of several risk assessment approach that exists. However, most of the risk assessment approaches have failed in addressing the context of the risk management process, how to overcome an attack, how to account for the human elements, evaluation and validation of data, probabilistic data and its improvement, and tool support. (Ten, Manimaran and Liu, 2010) proposed an implementation of a comprehensive cybersecurity framework with the help of the SCADA system for critical infrastructure. The key significant components that have been proposed for the framework include anomaly detection, real-time monitoring, impact analysis with the help of tree-based methodology and the application of mitigation strategies; the attack tree was designed on the effectiveness of the power system control networks to help in evaluating systems, scenario and vulnerabilities by identifying the adversary objectives in the system. Additionally, (Izuakor and White, 2016) suggested a novel approach for assessing critical infrastructure asset identification using a multi-criteria decision theory to address the difficulties of identifying crucial assets. The current methodology stops short of providing a systematic framework for making important decisions. (Bialas, 2016b) proposed a novel formal risk assessment approach for dealing with dangerous accidents' internal and external effects in sensitive infrastructure. This risk assessment approach adhered to the ISO31000/IEC31010 risk control and coordination standard. This study did not consider interdependencies, and it also did not have a framework for determining risk level and control mitigations. (Fekete, 2011) explained how society creates decisions over what is most relevant to them based on the amount of power society has. The study also shows how to classify what is most relevant to them, focusing on the assumption that there is no total defence from cascading effects and risks. The study of Fekete is less concerned with hazard reduction. European Telecommunications Standards Institute (ETSI) also analysed a telecommunication system by using UML to create a model for the telecommunication system named "Danger Vulnerability and Risk Analysis" (TVRA), which aids in strategic analysis of security targets, unexpected events, properties, vulnerabilities, and challenges (Virtualization, 2013). (Ezell, 2007) has proposed a concept that uses the Infrastructure Vulnerability Assessment Model (I-VAM) to quantify vulnerability and applied it to a medium-sized clean water scheme. His analysis, on the other hand, struggled to classify properties

and instead quantified the system's weaknesses. (Cherdantseva et al., 2016) conducted a study of the current state of cybersecurity risk management utilising SCADA systems. The study looked at the plurality of risk management methods that evolve or contribute in the framework of the SCADA method. They were evaluated and tool-supported in terms of their goals, implementation domain, risk management principles, effect assessment, and sources of probabilistic evidence. According to their findings, an intuitive scheme for categorising cybersecurity risk management approaches for SCADA systems has been proposed. Regardless of the various risk reduction methods for SCADA structures, the requirement for a holistic solution that includes all risk management processes remains unmet.

According to (Byres, Franz and Miller, 2004), they proposed applying the attack tree methodology on SCADA communication systems based on the standard MODBUS protocol attack. This type of approach offers a flexible and structural way of undertaking security analyses of applications, protocols, and networks. These authors identified some possible attack objectives that an intruder might attain against a MODBUS-Based SCADA system and the existing security vulnerabilities inherent in the SCADA systems. There are attack trees that are typically helpful tools used in modelling vulnerabilities and threats in different systems from their study. Nonetheless, a threat modelling valuable method to the protocol designers, vendors, and users' needs more attention. More formal approaches that enhance the aggregation of low node values and make dynamic reflection are needed.

Research by (McQueen *et al.*, 2006) showcase a new model used in estimating the time to compromise a system component that an attacker can access. Further, the model offers an estimate of the time-to-compromise's expected value as a function of identified vulnerabilities and attacker skill level. The model was used in aiding in risk reduction estimation between a baseline system and a SCADA system. The research by (McQueen *et al.*, 2005) shows that risk reduction on a partial SCADA system was carried out and a methodology to estimate quantitative risk reduction.

From the methodology that (McQueen *et al.*, 2006) discusses, it is poised as an effective way of estimating the time-to-compromise. (Sapori E, Sciutto M and Sciutto G, 2014) Proposes a risk-based methodology assess security management systems that were applied to railway infrastructure. The methodology analysed the system, integrates technological, human and procedural aspects by using flow charts. It analysed how to manage and identify threats, vulnerabilities and criticality of the subsystems. However, human functions replaced with technological systems are not a constantly achievable goal. Also, identifying critical assets were not the main focus of this paper.

In (Islam *et al.*, 2017), there is an illustration of a risk management framework that helps users with cloud migration decisions, following the necessary risk management principles. This framework is essential as it enables users in identifying risks based on the relative importance of migration objectives and risk analysis with the semi-quantitative approach. In the end, the users can make

accurate cloud migration decisions based on the critical migration scenarios. Practical risk assessment approaches are the cornerstone of a successful application of a critical infrastructure protection program. Different risk assessment approaches for critical infrastructures supports this insinuation. Risk assessment is thus indispensable to identifying threats, assessing the vulnerabilities, and evaluating the impact on infrastructures, assets, or systems considering the possibility of the occurrence of these threats. This is one of the critical elements that differentiate risk assessment from a traditional impact assessment approach. Studies by (Theocharidou and Giannopoulos, 2015); (Adar and Wuchner, 2005) discuss critical challenges facing critical infrastructure risk management and outline several methods and best practice guidelines that encompass creating frameworks, risk analysis methods, and the adoption of models. The sole focus on technical threats and technical solutions are no longer adequate. Therefore, security and risk management methodologies have to consider societal factors (Schauer, 2015). Risk management is applied to threats and hazards of all kinds that affect critical infrastructures and how best to lessen those threats and hazards based on current capabilities and resource requirement (Committee, 2010).

### **2.5.2. Frameworks/Standards/models for critical infrastructure**

Different internationally accepted risk management standards such as ISO 31000 (ISO, 2009) offer risk management approaches that consider risk management crucial in comprehensive organisational processes, including management processes and strategic planning. IEC 31010 is also another recognised risk management methods and techniques(GOST, 2009). NIST framework focuses on managing cyber-security risk and NERC CIP to identify and protect the critical cyber-assets that back up the electric power grid's dependable operation. According to (Cybersecurity, 2014), the NIST framework is considered a practical approach to managing cyber-security risks. It is applied in delivering a complete platform that helps identify relative paths, providing guidance that ranges from requirements to implementation. The critical infrastructure organisations can leverage the NIST framework's application and their existing frameworks to enhance a systematic identification, management, and assessment of cybersecurity risks. NIST framework can also serve as the foundation for a new cybersecurity program or a mechanism that improves new programs. The consequence of using this framework serves as the groundwork that encompasses a reassessment to make a verification that helps to fulfil the cybersecurity requirements (Purdy, 2010).

There are guidelines, such as the North American Electric Reliability Company (NERC), that have recognized the cyber-security principles for critical infrastructure protection (CIP-002 to CIP 009) to include a security mechanism for the documentation and security of critical cyber assets that maintain the electric power grid operating continuously (NERC, 2006). The National Institute of Standards and Technology (NIST) established the cyber-security charter to enhance a country's essential infrastructure (O'Rourke, 2017). NIST includes a risk management system to enhance network compliance, reinforce risk management procedures and ensure institutes' execution. A particular goal-

driven risk management approach (Islam et al., 2017) accentuates goals as objectives specific to the organisation mission. Risks are reflected as a hindrance to the goal, so that identified risks are assessed based on which goals they oppose. The method is helpful in various domains, such as cloud computing and software development.

NIST SP800-30 risk assessments uphold risk response resolutions at the different levels of the risk management order. The Tiers focus on the organisational operations, assets and individuals and select standard controls (Stoneburner, Goguen and Feringa, 2002). The Centre for Internet Security Critical Security Controls (CIS\_CSC) provides a prioritised set of actions that alleviate the most coordinated attacks against systems and systems and can be applied for critical infrastructure sectors. OWASP methodology helps organisations estimate risk from business and technical perspectives (Tymchuk, Iepik and Sivyakov, 2017). A common weakness scoring system (CWSS) provides a mechanism for prioritising software weaknesses in a dependable, simple, and open way. It is a standardised approach for characterizing weaknesses, thereby allowing organisations to make more informed decisions during the risk management phase and give higher risks (Martin, 2007). ENISA, the European Union Agency for Network and Information Protection, has established a mechanism that requires information regarding asset security to be ensured (Luna *et al.*, 2011). STIX model represents structured threat information, which conveys the full range of CTI (Barnum, 2012). STIX is actively being adopted or deliberated for adoption by cyber threat-related organisations, which helps organisations understand the proper context of threats to make smart defensive choices.

The Industrial Automation and Control Systems Security (ISA99) (Piggin, 2013) committee tackle cybersecurity issues regarding industrial automation and the control of systems through the Industrial Automation and Control Systems Security/International Electrical Commission (ISA/IEC-62443) standards

### **2.5.3. Machine learning Technique for Risk prediction**

This section introduces the fundamental concepts and principles of machine learning as it applies to critical infrastructure systems. We explore machine learning approaches and best practices for designing, building, and evaluating machine learning applications in critical infrastructure. (Ahmed and Abraham, 2015) In recent years, with cloud computing developments, there are risks involved with using a cloud environment. The researchers applied different selection algorithms such as random filter classifiers and isotonic regression to assess risk assessment. The results showed that prediction algorithms and feature reduction are very efficient and can help achieve high-risk modelling accuracy. Future research could focus on integrating machine learning models to isolate risk factors in private and public network infrastructures. (Bilge, Han and Dell'Amico, 2017); in this paper, the researchers found that the current evolution of cyber threats ecosystems whereby no system can be considered invulnerable. It is critical to quantify risks levels within a system and develop risk

prediction methods so that proactive measures can be taken to minimize the damage of cyber threats. The researchers presented the Risk Teller system, which helps to analyse binary file appearance logs of machines to make prediction of which machines are at risk of infection months in advance. They show that Risk Teller can also use the machine profile computed for a specific machine to enhance the prediction of subsequent infections with the highest prediction precision.

(Fang *et al.*, 2019) Forecasting and predicting cyber threats are critical. Previous researches have shown that cyber-attack data exhibit some phenomena such as high nonlinearity that become challenging in predicting cyber-attack risks and modelling the risks. The researchers utilized a deep learning framework with bi-directional recurrent neural networks to assess the magnitude of risks. The study showed that bi-directional recurrent neural networks with long short-term memory (BRNN-LSTM) have a high significant prediction accuracy compared to the statistical method. Future research should look into the application of machine learning to detect software vulnerabilities. (Gupta *et al.*, 2020) With recent technological advancements and especially in intelligent devices, traditional data analytics fail in handling big data generated by different devices. The researchers explored machine learning and deep learning models to make intelligent decisions concerning attack identification and mitigation. They proposed ML-based secure data analytics architecture (SDA) to help classify attack input data. The threat model address research challenges in SDA using different parameters such as reliability, accuracy and latency. In the future, more research should focus on understanding the existing SDA proposals concerning parameters and how they can be aligned to cyber-security threats. (Husák *et al.*, 2018) This research provides a survey of prediction and forecasting methods applied in cybersecurity. The researchers discuss four main tasks: attack projection, recognition of intention, the prediction of next moves, and intrusion prediction. The authors proposed attack graphs, Bayesian networks, and Markov models to help in learning the risks and threats. They further discussed the application of machine learning and data mining in threat detection. The results indicate that suitability for machine learning is needed to understand risk and intrusion predictions. Future research needs to focus more on improvements in attack prediction and its utilization in practice.

(Liu, Zhang, *et al.*, 2015) This research offers the first step to understanding how it is possible to predict cybersecurity incidences with machine learning techniques and use externally evident malicious activities directly associated with network entities. To test their hypothesis, the researchers collected IP address-based host reputation blacklists. Their hypothesis testing features are also shown with features to support vector machine (SVM) for prediction. The results show that it is possible to achieve a reasonably good prediction performance over the forecasting window. Future research should focus on the effectiveness of machine learning in reducing risks at the critical infrastructure level. (Liu, Sarabi, *et al.*, 2015) In this study, the researchers characterize the extent to which cybersecurity incidents can be predicted based on an externally observable properties organization's

network. They collected externally measurable features related to an organization's network from mismanagement systems and malicious activity time series. They then train and test a random forest (RF) to assess the vulnerabilities. The results indicate that cyber incident forecasting offers a completely different set of characteristics than detection techniques. Future research should focus on predicting incident type and how to generate risk profiles based on an organisation's network infrastructure.

(Lilly *et al.*, 2019) Despite significant advancements in identifying, deterring, and mitigating cyber incidents, NATO agencies are discontented, along with the intelligence agencies whose strategy against cyber incidents is primarily reactive and implemented rather than being executed before attacks. The researchers have proposed an indications and warning (I&W) framework for the cyber-domain by applying this framework and examining its effectiveness in the private sector and also deployed it on an actual case. The research finds that indications and warning frameworks effectively detect cyber threats and risks even before they occur in the private sector infrastructure networks. Future research should close the gap and increase understanding of how governments can apply this framework and integrate it within the existing processes.

(Makawana and Jhaveri, 2018) With the world's information being shared using the Internet, cybersecurity has been a problem. Machine learning techniques are applied in dealing with cybersecurity threats. The researchers found that machine learning for cybersecurity has significant potential in enhancing network safety. The results also showed that machine learning is an integrated way to protect their data in real-time. Future research should discuss the effectiveness of machine learning in critical infrastructures in the public sector. (Okutan, Yang and McConky, 2018) If the cyber-threats are predicted a reasonable amount of time before their occurrence, there could be proper defensive actions taken; mostly, there lack enough observables of malicious activities. This research suggests the application of unconventional signals derived from various data sources with variant time granularities to help predict cyber incidents. They proposed a Bayesian network to help in predicting cyber-attacks. The results show that depending on the granularity, and the unconventional signals can predict cyber-attacks. Future research should discover more how the sampling approach can be used together with the Bayesian network to predict and assess risks in critical infrastructures. (Ovelgönne *et al.*, 2017) despite the growing speculation concerning the role of human behaviour in machines' cyber-security, there have been gaps in concrete data-driven analysis and evidence. The researchers used the Worldwide Intelligence Network Environment (WINE) platform to study 1.6 million machines to understand the relationship between cyber-attacks and user behaviour against personal computers. The results showed a strong relationship between the number of attempted malware attacks and several features. They also show that software developers are at more risk of engaging in risky cyber-behaviour than other categories. In the future, more focus should be on how these software developers can approach machine learning as a way of protecting their system from external

threats and cyber-attacks. (Papernot *et al.*, 2016) in this research showed that advances in machine learning had enabled different applications, such as autonomous systems and data analytics. Machine learning has been argued to contribute to exposing new vulnerabilities in software systems. They identify key insights that result from related structural elements of machine learning algorithms. The research concludes that exposing the relationship between resilience and model accuracy is key applicability of machine learning. In the future, more research should use models to understand the complexity, resilience and accuracy that must be calibrated for the safety of network infrastructures.

(Singh *et al.*, 2020) Presently, machine learning techniques are used to understand 5G network infrastructures with the emerging IoT and 5G infrastructures. The researchers find that it is possible to deploy power-optimized technology in a way that promotes the network's long-term sustainability. They propose a machine learning-based network sub-slicing framework in a sustainable 5G environment to optimise the network load balancing issues. The results show that machine learning techniques effectively understand the criticality of the 5G network infrastructure and the threats attached. Future research should focus on using machine learning to enhance the stability and sustainability of network infrastructures. In (Sun *et al.*, 2018) article, the researchers argue that driven by increasing scale and high profile cyber-security incidents related to the public data, there has been a paradigm shift in understanding and defending against cyber threats. Machine learning is one way to do it. They propose cybersecurity incident prediction schemes by utilizing different data sources, including the organization's reports and datasets, synthetic data, and social media data. They find that customizing models to assess risk can help characterise the latency and serve as an important way to align future research. Future research should focus on forecasting incidents with high accuracy and without making data assumptions.

(Tanwar *et al.*, 2019) In recent years, the emergence of blockchain technology has become a trending, disruptive and unique technology. Blockchain technology raises security issues such as double-spending and majority attack. To handle issues, data analytics is necessary for blockchain-based secure data. Machine learning was proposed to improve the system's accuracy and provide precise network results and resilience against attacks. The researchers find that machine learning and blockchain technology can be used in intelligent applications such as Unmanned Aerial Vehicle (UAV) and smart cities. Future research should consider the issues and challenges in risk management and assessment in blockchain technology. (Tolubko *et al.*, 2018) This research is typically about the definition of cyber threats in the information system. Cyber threats lead to significant loss of network resources and lead to system disability as a whole. The most critical task in an information system network is network monitoring. This research sought to develop a method to detect cyber threats and develop countermeasures, especially machine learning implications. Their research found that different methods allow the network layers to initiate topology re-arrangement to interrupt cyber-

attack paths. Future research should uncover the effectiveness of machine learning and the OSI model in facilitating network security risk assessment.

(Varshney and Alemzadeh, 2017) Machine learning algorithms influence the way we make decisions and our interactions daily. As we consider critical infrastructures' safety, this research argues that it is vital to take machine learning into account. The researchers define machine learning and its integration to safety and harm created by unwanted outcomes. They found that the foundational principle of empirical risk minimization, statistical machine learning lacks a sufficient objective. Future research should consider the interpretability and causality of predictive risk assessment models and approaches beyond human involvement. (Veeramachaneni *et al.*, 2016) In this research, they presented an artificial machine learning approach, an analyst-in-the-loop security system where Analyst Intuition was put together with state-of-the-art machine learning helped build a complete end-to-end artificially intelligent solution (AI). The system was found to present features such as a big data behavioural analytics platform, an outlier detection system, a mechanism to acquire feedback from the security analysts, and a supervised learning module. The system was validated using a real-world data set, and the results showed that the system is capable of learning to defend it against unseen attacks. Future research should focus on an in-depth integration of analyst-driven solutions to prevent cyber threats. (Xu *et al.*, 2018) increasing an understanding of the evolution of threat situations, analysing cyber incident data is essential. The researchers report a statistical analysis of a breach incident data involving cyber hacking activities such as malware attacks. The study shows that breach size and hacking breach incident interval times need to be modelled with stochastic processes instead of distributions as there are autocorrelations. They propose models to fit inter-arrival times and breach sizes and show that models can predict the breach time. Future research should analyse the threat and magnitude of cyber threats and use machine learning models to ascertain the risk imposed by autocorrelations.

(Xu, Hua and Xu, 2017) Internet-based computer information systems are essential in modern society, but they are threatened by cyber-attacks that can cause critical risks. It is vital to measure and predict how effective the cyber defence mechanisms are to initiate the systems' defence. The researchers investigated how to predict and measure the effectiveness of a cyber-defence mechanism (early-warning). They proposed a new vine copula model that helps in predicting the effectiveness of early warning more effectively. They also present a discussion of how to use the prediction approach in practice. Future research should consider the alignment of machine learning and the early warning system to assess risks in rotationally symmetric dependence structure.

#### **2.5.4. Case Study**

Proposed in (McQueen *et al.*, 2006), a model can be applied in estimating the time to compromise a system component that an attacker can easily find. The model was applied in a case study to aid the

risk reduction in a small SCADA system comprising eight generic module types connected to a local Ethernet LAN. The total number of system vulnerability was reduced to a certain level. Proposed in (Bialas, 2016b), a novel designed risk management approach entails dealing with external and internal impacts of risky event that occurred in the critical infrastructure. However, this is a method that is only embedded in the resilience process of critical infrastructure. These are only requirements that can only be implemented on the ready-to-use software platform for further experiments. The results of the experimentation are used as the CIRAS input. The tool applied to the risk reduction component in CIRAS and the validation process considered the basis for elaborating project uses cases. The paper presented the validation experiment related to risk management in critical infrastructure using the ready-made OSCAD software platform and performed a case study to acquire knowledge.

Presented in (Ten, Manimaran and Liu, 2010), there is an in-depth survey on critical infrastructures cybersecurity. A SCADA security framework that has these four distinct components is proposed: Real-time anomaly detection, monitoring, impact analysis, and strategies for mitigation. Further, an attack-tree-based impact analysis methodology is advanced. This is based on power system control networks, and it is mainly deployed in understanding system evaluation, scenario, and vulnerabilities at the leaf-level by identifying the system's adversary objectives. The methodology is also applied in study cases to help identify the adversary objectives of the system and identify access points of the power system control networks and evaluate the vulnerability of the network and proposed in (Sapori, Sciutto and Sciutto, 2014) the implementation of risk-based approaches in use by process engineering to achieve a quantitative assessment of the security management systems. This is a methodology that is exposed and applied to a railway case study. Primary steps guide system analysis (the study of macro operability functions, identification of subsystems) and ways to integrate human, technological and procedural aspects using flow charts. The later steps describe ways to manage threats, vulnerability and criticality of critical infrastructure subsystems, identify “primary causes” and “top event consequences” drawing event and fault trees, and finally the calculation of residual risk for the security management system. Thus, the methodology is applied on a case study of one railway subsystem and the results of the quantitative risk analysis are exposed.

#### **2.5.5. Determining Asset Criticality**

In (de Gusmão *et al.*, 2018), the authors proposed a model that integrates fault tree analysis, decision theory and fuzzy theory to ascertain the current causes of cyber-attack prevention failures and determine the vulnerability of a given cybersecurity system. However, predicting risk type within a risk management framework is not the focus of this paper.

(Izuakor and White, 2016) proposed a new approach for critical infrastructure asset identification using multi-criteria decision theory to resolve the challenges of identifying critical assets. The approach didn't provide a systematic process for arriving at criticality

decision. (Fekete, 2011) described how society gets to choose what is critical to them, based on how much influence it has on them. Shows how to identify what is critical with regarding the fact that there cannot be full protection with respect to cascading effects and threats. The paper focuses less on threat prevention rather than the impacts of threats. Strategic proactive planning, the purpose of civil protection and activities of risk management are among the key attributes of identifying the above. In (Alidoosti *et al.*, 2012) the main purpose of this article is to present a new methodology based on the RAMCAP framework and fuzzy inference system (FIS) to provide a structured framework to build a more secure, safer and more reliable critical infrastructures in order to develop, implement and control systems and sub-systems.

There are several contributions that justify the necessity and importance of identifying critical assets and vulnerabilities of the assets of critical infrastructure. However, we have made several observations. In particular, there is a lack of systematic approach that supports critical infrastructure organisation by identifying critical assets and their relative vulnerability.

## **2.6. Challenges faced by critical infrastructure systems**

Like any other complex system, a critical infrastructure system is composed of distinct elements with different significance levels, categorized into several levels and others are interconnected through linages of various intensity and types. An integrated structural arrangement leads to a broader correlation between the individual subsystems, which help determine the intensity and how the propagation of critical infrastructure systems failures affect society (Ghorbani and Bagheri, 2008). A study by (Leita and Dacier, 2012) showed that several issues need to be considered before complete protection of the critical infrastructure systems is initiated. As far as the risks are concerned, there are fundamental security risks directly relative to critical infrastructure systems, manifested in logical, physical and technical defects in the network infrastructure. The research has grouped these by (Leita and Dacier, 2012)as:

- Human error
- Failure of technical hardware
- Technical obsolescence
- Deviation from the quality of standard service
- Application/protocol attack
- Well thought out act of information extortion
- Distributed Denial-of-Service attack
- Botnets
- Web interface attack

- Advance persistence or state-sponsored threats

Other threats will involve ransomware, water hole attack, dropper, rootkits, spyware, worms, Trojan horses, phishing and spear phishing. (Levy-Bencheton and Darra, 2015) On account of ENISA, identified and recorded various threats that could apply within a wide range of industries. They include:

- Physical and large-scale attacks stem from intentional action and could affect any component by disrupting, altering, exposing, or gaining unauthorized access. Real-world cyber-attacks with destructive results have taken place in the past on another domain of interest, and more specifically on the Ukrainian power grid infrastructure (Shehod, 2016).
- Insider threats include malicious actions. The threat-actor always originates from the organisation itself.

Threats to critical infrastructure are real as the restructuring process has changed the networks' reliability and the services provide. This has created several critical infrastructural protection violations that range from stealing electronic data, altering or destroying electronic information on networks, and manipulating physical critical infrastructure systems and equipment through organizational controlled networks. When this happens, it collapses the mobility risks, and boundaries for the countries as the world is technically connected (Mikhalevich and Trapeznikov, 2019). The critical infrastructures are connected through information technologies as data are transmitted through the application of information highway. This implies that security measures to safeguard the data in critical infrastructures from attackers are highly needed. The critical infrastructures security concept is conveyed in the form of cyber-dependent attacks that range from intrusions into computer network space, and this is the primary mode of attack that varies in scope.

When attacks are propagated against critical infrastructure systems, these attacks have critical and detrimental effects on the national and general lifestyle. This implies that the critical infrastructure's success depends on identifying risks and creating meaningful relationships between the stakeholders who are on the front line to make sure that the critical infrastructure systems are safeguarded. The government's responsibility ranges from the identification of the risks to the aspects that lead to the failure of the critical infrastructure systems. To manage this, governments take measures to consider issues such as human error, equipment failure, and the natural causes that might impact the effectiveness of the critical infrastructure systems and lead to losses across the society.

### **2.6.1. Evolving Cyber-threat landscape**

A critical infrastructure system's functioning is under different threats, especially by a wide range of security threats. These threats can be classified into:

- Technology threats: These pertain to the technological emergencies that might include the widespread disruptions by radiation emergencies, widespread effect on engineering works, air, road, and traffic accidents.
- Climatological threats: These include natural disasters such as heavy snowfall and floods.
- Biological threats: These might include pandemics
- Geological threats: These include landslides, earthquakes, and volcanic activity
- Criminal threats: Such as criminal activity, terrorism, and armed conflicts.

Depending on the threat category, some emergencies usually lead to individual failures, which can typically occur in a critical infrastructure system. Once the threats have been generated, they can propagate further within the critical infrastructure system, and they can eventually lead to the production of negative impacts within a critical infrastructure system and increase the intensity and the effect (Hurst, Merabti and Fergus, 2014). The system failures in critical infrastructure produce effects within the critical infrastructure system and also outside the system where they can specifically affect the society on the ground of national interests such as the basic societal needs, state security, and the economy in general (Rinaldi, Peerenboom and Kelly, 2001). The advances in automated technology, such as the Internet of things, sensors, and cybersecurity measures, can assist the people responsible for protecting critical infrastructure more efficiently. With the help of these advances, they can efficiently understand the potential threats, undertake system diagnostics make predictions for possible changes in the critical infrastructure systems, and strengthen the security and the resiliency of the critical infrastructure systems (Kozik and Chora, 2013). In countries such as the United States, the department of security makes sure that it has taken measures to put in place targeted solutions for critical infrastructure systems safety and resilience across multiple sectors.

## **2.6.2. Adopting Machine Learning Techniques**

ML models are sort of elaborated than outmoded programs because they deal with a set of complex data. Tactical design verdicts must be made before models getting taught. The risk associated with machine learning will show in nearly all life cycle stages, beginning from envisaging to implementation. Improvements to the authentication frameworks have to shield almost all life cycle levels as they occur traditionally, with the additions highlighted below.

### **2.6.2.1. Transparency and Interpretability**

ML models are usually be viewed in terms of its inputs and outputs, and have so many complex decision-making layers, making appraisal and application traceability quite challenging. ML-powered applications are sometimes supposed to be transparent. Organisations usually want to notice how the data is being processed to ensure decisions. To minimise the risks, the ML model's transparency and interpretability have to be placed and assessed in high order.

### **2.6.2.2. Feature Engineering**

ML models are designed to recognise patterns from the data, and the data is usually complex. Data becomes complex due to its quality and nature, mostly with unstructured data. Feature engineering is usually needed to convert the unstructured data to a structured one before processing. These processes are also in quick makeovers and complex with custom packaging as they have the capability of different engineering transformations of the data for models assessments. As they develop complexity, the risk assessments likewise have to be carried out.

### **2.6.2.3. Data Quality Control**

A key difference that distinguishes traditional application and machine learning application is the capacity to study patterns from the data. Traditional applications are destined to the programmed path and cannot change once arrayed. Machine learning prototypes are adept at considering data insights and act accordingly. This behaviour demands quality and new data; otherwise, the algorithms will not deliver the projected accuracy. If silos exist in the CI, it could limit or block such quality data and weaken the applications.

## **2.7. Summary**

An overview of the primary risk management, CTI, and machine learning for risk prediction approaches to develop a common understanding of the research domain is presented in this chapter. A particular emphasis was placed on emerging risk management issues that were considered challenging, most notably the need for CSRM to recognise the importance of implementing CTI and a machine learning framework for automation of risk type prediction issues. Additionally, the chapter presents some elements for cybersecurity risk management in critical infrastructure. The chapter further discusses how existing methods affect cybersecurity risk management in critical infrastructure. The related literature on risk management methodologies for critical infrastructure and machine learning approaches for risk prediction were carefully defined. Existing works in these areas are taken into account since one of the significant issues in risk management is the lack of comprehensive cybersecurity risk management that considers the adoption of CTI and machine learning for risk prediction for critical infrastructure protection. It is also necessary to identify the assets and their criticality for critical infrastructure to identify these assets' threats and vulnerabilities. Cybersecurity risk management is a nascent field, and the theoretical frameworks are yet to be recognised. The multifaceted and varied nature of the cybersecurity domain has meant no easy theoretical fit from mathematical, science or other areas. The prevailing attempts to provide a theoretical model are mainly complex and involve significant computational work. This research intends to fill these gaps and proposes an integrated cybersecurity risk management framework for critical infrastructure. Other

gaps in the research include the researchers' inability to evaluate the risk level for critical infrastructure.

## **CHAPTER THREE**

### **RESEARCH METHODOLOGY**

#### **3.1. Introduction**

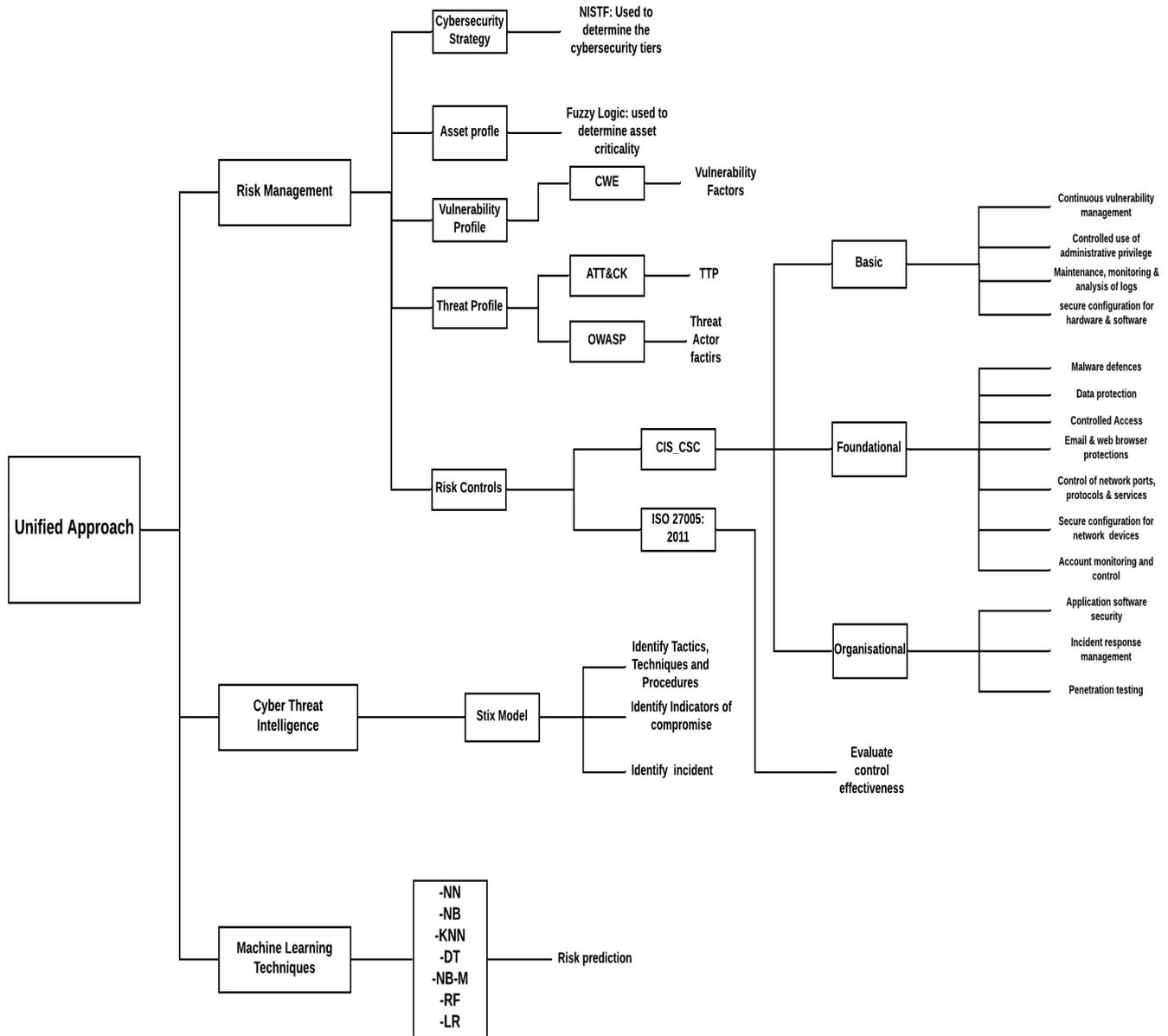
This chapter details the research methodology adopted in this thesis to address the research questions outlined in chapter one, guided towards integrating a CSRM framework for critical infrastructure. A research methodology is a critical element of research studies that are used to classify current challenges and, as a result, achieve the goals of a specific research project (Kothari, 2004). It is a tool for collecting reliable data and doing a rigorous study to obtain the correct information. The research approach defines the study's goal and specifies the criteria relevant to the research needs (Neuman, 2013). According to (Mackenzie and Knipe, 2006), study methodology identifies how research design tools and procedures should be utilised, distinguishes between approaches and findings, and emphasises the significance of clarifying and achieving the research goal. In general, the study methodology aims to have a good idea of the approaches or procedures used to solve the research problems.

As a result, the analysis tool determined for this thesis is to provide an i-CSRSM framework for critical infrastructure while assessing the quality of work conducted and the nature of the different approaches. The researcher conducted a systematic literature review (SLR) to achieve this objective. Lastly, the researcher evaluated the proposed framework in a real-life case study. The case study comprises distinct characteristics that demonstrate the broader scope of the proposed framework. A research methodology must be followed to achieve this research's objectives, address the research questions outlined, and validate the research framework effectively. This chapter presents the methods and hypotheses used to establish the proposed i-CSRSM framework and the analysis methodology used to validate its applicability.

### **3.2. Methodology for Framework Development**

The framework development process takes into account industry standards, theories, and methodologies. Figure 3.1 illustrates the steps included in the framework development methodology. Step one narrates the gaps in the existing literature, step two and step three proposes a novel framework to address the problem domain and step three evaluates the proposed framework using a case study.

An overview of the different standards, frameworks, and models and the features or aspects derived from them that make it a unified approach is provided in Figure 3.1.



**Figure 3.1:** Unified Approach model to i-CSRSM that leverages existing industry standards to assist organisations in attaining risk management by ensuring that every step and activity is performed according to generally accepted security principle.

### 3.2.1. Step 1: Literature Review

The proposed research methodology's main objective is to identify, summarise, and analyse all approaches that have been proposed or used to represent risk management in critical infrastructure. The first step in developing the methodology is to review the current literature, i.e. to define, examine, and summarise the current state of the art literature in this field of study. In achieving this, a systematic review (SLR) is conducted. A systematic review is a well-defined and methodical way to

identify, evaluate, and synthesise the available evidence concerning a particular technology to understand the current direction and status of research or provide a background to identify research challenges (Keele, 2007). The SLR use creates a path that makes the review's scope definite to other researchers and makes sure that the identified literature is relevant to the study. Data from the literature outline the different approaches used in developing the i-CSR framework in addressing research questions, aims and objectives. Combining these techniques allows us to systematically identify available evidence on risk management for critical infrastructure from academic and industry works. This method was chosen because of the requirement to have a credible, repeatable and fair evaluation of the available studies assessing risk management on critical infrastructures.

### **3.2.2. Step 2: Development of Framework and Process**

This step entails developing an i-CSR framework that incorporates various concepts, a unified process that integrates CTI information and ML techniques to support risk management activities in critical infrastructure. Also, the cybersecurity risk management tool (i-CSRMT) that supports performing risk management. The process outlines various activities that every organisation could use to achieve a comprehensive view of threats and associated risks. Various techniques, theories, and standards have been used to ensure that the framework is designed and applied following universally accepted principles. By taking sections from renowned industry standards, guidelines, frameworks, and models and implementing them across various activities were implemented across different activities within the process.

The process consists of five different sequential activities, which serve as a manual for developing an efficient i-CSR framework for critical infrastructure. These activities are linked with each other, and every activity includes steps to support specific task relating to i-CSR and guide organisations in making critical decisions. Each activity's output is used as the input for the next one. The following sections provide an insight into the models and standards used:

#### **3.2.2.1. Cyber Threat Intelligence (CTI)**

For organisations to respond to their specific threats and make informed decisions on which countermeasures to deploy, they must have detailed threat information. Therefore, we consider STIX the most widely used CTI method for the specification, capture, characterisation and communication of standardised cyber threat information.

- **STIX model:** STIX model represents structured threat information, which conveys the full range of CTI (Barnum, 2012). STIX is adopted to help organisations to understand the true nature of threats to make intelligent defensive decisions. For a valid defence against current and future threats, it is necessary to understand the threat actor's behaviour, capability in tactics, TTP and the threat actor's intent. Therefore, we adopted some of the STIX concepts

such as TTP, threat actor, indicator and incident and integrated them with i-CSRМ concepts to improve the i-CSRМ framework in CPS.

### 3.2.2.2. Industry Standards

We consider existing, widely used standards, guidelines, methodologies, framework, models, and practices to develop the framework. They include:

- **ATT&CK (adversarial tactic, techniques and common knowledge)** framework developed by MITRE is used for documenting common TTP used to target, compromise and operate in an enterprise network. We considered the ATT&CK framework so that the organisation's actors can gather valuable insights into the threat that can affect the organisation.
- **Common Weakness Enumeration (CWE)** is used for communicating the impacts of vulnerabilities. It introduces a common weakness scoring system (CWSS) which provides a mechanism for prioritising software weaknesses in a consistent, flexible, and open manner (Martin, 2007).
- **Open web application security project (OWASP)** provides basic techniques to protect against web application security challenges. To ensure consistency and relevance of risks and their impact, we adopted the OWASP risk methodology (Tymchuk, Iepik and Sivyakov, 2017). This methodology helps organisations to estimate risk from business and technical perspectives.
- **The Centre for Internet Security Critical Security Controls (CIS\_CSC)** is a collection of controls that help organisations protect their assets. It consists of sufficient controls that organisations may use to prevent or minimise identified threats and enforce a clear protection policy.
- **CAPEC** provides a comprehensive list of a known pattern of attacks employed by an adversary to exploit known cyber environment weaknesses. This relevant model has been adopted for threat analysis for effective cybersecurity.

### 3.2.2.3. Use of Machine Learning Techniques

Machine learning classifiers are widely used in several application domains such as text categorisation (Sebastiani, 2002), internet traffic classification (Posch and Nguyen, 2012), recommender systems (Yavanoglu and Aydos, 2017), and malicious “uniform resource locator (URL)” detection (Sahoo, Liu and Hoi, 2017). An accurate prediction can help organisations detect frequent cyber-attacks, affected assets, risk type, and relevant controls with machine learning classifiers. Therefore, we used well-known classifiers such as KNN, NB, NB-Multi, NN, DT, RF, and Logistic Regression for risk prediction.

### **3.2.3. Step 3: Research Validation**

To evaluate the main contributions of this research, an empirical research method is selected. The empirical analysis is growing in popularity in the information systems research domain (Runeson and Höst, 2009) because it is a valuable research tool for collecting relevant data for researching a complex information systems topic. As a consequence, a case study is chosen for this study. A case study is a technique that focuses on identifying the complexities that occur within a particular environment (Eisenhardt, 1989). Since it illustrates research initiatives and acts as a framework for creating well-structured research results, the case study methodology is commonly utilised in research domains (Straub, Boudreau and Gefen, 2004). The explanation for using a case study for this analysis is to provide concrete input on the validity of the i-CSR system and stakeholder viewpoints on the efficacy of using ML techniques to enhance the overall protection of critical infrastructure.

#### **3.2.3.1. Technology Acceptance Model and Unified Theory of Acceptance and Use of Technology**

We use the renowned Application Acceptance Model (TAM) (Davis, 1989) and the Unified Theory of Acceptance and Use of Technology (UTAUT) in developing and assessing the questionnaire used to gather feedback from stakeholders (Venkatesh et al., 2003). TAM is concerned with predicting a newly created information system's adaptability by users within an environment to evaluate its acceptability to a context and the changes that may be made to make it applicable to all users. According to the authors, two main factors decide any information system's acceptability: perceived ease of usage and perceived utility. The degree to which an individual assumes that using a device can increase his success is referred to as perceived usefulness (Davis, 1989). The degree to which a person assumes that using a device can increase results is referred to as perceived ease of use. UTAUT, on the other hand, suggested four constructs: contextual impact, success expectancy, commitment expectancy, and encouraging environments, which are direct determinants of purpose and behaviour consumption (Karahanna and Straub, 1999). As a result, TAM and UTAUT were chosen because their structures tend to have some partnership for analysing feedback.

### **3.3. Research Approach**

Choosing an effective research method is essential for any research study. The study methodology is the systematic application of several steps for data collection, examination, and comprehension to elicit concrete observations and conclusions (Amaratunga et al., 2002). According to (Orlikowski and Baroudi, 1991), it is essential to specifically grasp the purpose of analysis to assess and choose an appropriate strategy for achieving the goal. They went on to say that when choosing a research methodology, two considerations must be considered: the characteristics of the research subject and the time required to perform the analysis.

### **3.3.1. Qualitative research approach**

The qualitative analysis technique examines social phenomena and helps the researcher perceive and establish a detailed interpretation of the research results (Lewis, 2015). The qualitative research methodology, according to (Silverman, 2016), allows for the use of various strategies such as case study, assessment, and interview to analyse the subject and provide a detailed description of the issue. Therefore, we implement the use of a qualitative analysis methodology as it helps the researcher link issues to the real-life case study.

### **3.3.2. Quantitative research approach**

Quantitative research is systematic because it assesses research phenomena in numerical values (Kaplan and Duchon, 1988). The quantitative method allows for examining various variables and their relationships in a specific sense (Burns, 2000). A questionnaire, which includes a collection of specific questions and responses, illustrates a quantitative methodology analysis tool to obtain data. The data obtained for the questionnaire is evaluated statistically, and the conclusions are made available. In the case of i-CSR for critical infrastructure, which is dependent on customer approval and implementation, a quantitative method is used to determine the variables that influence the organization's adoption decision.

### **3.3.3. Mixed Research Approach**

The integration between qualitative and quantitative approaches is known as mixed methods, and conclusions were drawn using both approaches (Östlund et al., 2011). A mixed-method approach can produce a concrete outcome as it combines an 'analytic' approach to understand variables (quantitative) or a 'systemic approach to understanding the interaction of variables (qualitative). In addition to a mixed-methods approach, (Malina, Nørreklit and Selto, 2011) claimed that using multiple methods and sources of data collection aids in producing ample evidence to address the research questions. A mixed method methodology enhances and maintains the efficiency of any study by using multiple techniques such as interviews and questionnaires. Using hybrid approaches, diverse forms of data are obtained from different outlets, which enhance and strengthen the data and conclusions' reliability.

### **3.3.4. Adopted Research method for this research**

A mixed-method approach is considered for this research because it allows for qualitative and quantitative analysis, enabling a researcher to explore critical aspects and confirm quantitative analysis findings. This research focused not only on applying theory but also on testing the applicability of a framework and answering whether the proposed framework can improve cybersecurity risk management for critical infrastructure. The mixed-method methodology helps the study

be more diverse in terms of data collection and interpretation and draws conclusions and relating the results derived from the various data collection approaches (Creswell and Creswell, 2017).

Also, various research techniques associated with qualitative research approaches were used to ensure rational research outcomes. The case study was considered to evaluate the practical implementation to a real-world scenario and guide the verification of i-CSR framework validity and ML techniques' usability.

### **3.4. Research Design**

The development of related procedures and descriptive theory to enable stakeholders to evaluate the i-CSR framework in an organisation with critical services is the focus of this research. The Research design that offers a transparent picture of the research structure, including data collection techniques, research queries, and data sources used in performing the analysis, is referred to as research design (Denzin and Lincoln, 2002). The study design is determined by the type of study conducted to obtain quantitative outcomes or through an action plan that involves a series of exercises and activities based on the research questions to obtain results and conclusions (Maxwell, 2012). A study design allows a researcher to detail many of the research methods, such as choosing an appropriate testing methodology (Lewis, 2015). The following criteria's were considered in establishing the research design:

- In testing the practicality and relevancy of the framework, the researcher was involved directly,
- A critical infrastructure domain was selected for testing the applicability of the proposed framework,
- Guidance on how to apply descriptive theories,
- In evaluating the practicability of the proposed framework, experienced stakeholders were involved.

This research aims to examine risk management's role in critical infrastructure and how the framework can help organisations improve their risk management practices. An outline of the overall research design methodology used in this research is shown in Figure 3.12. The research architecture is divided into four main phases, each with its collection of activities. Firstly, a review and analysis of the existing literature within the problem domain is carried out to identify the knowledge gap. The second step is to build the i-CSR framework to solve the research problems. The third step is associated with the techniques for testing and validating the proposed framework. The limitation of the study and future research work is concluded and presented in the last step. The four stages are presented as follows:

#### **Stage 1- Identifying current risk management practice**

By reviewing the literature, state of the art in risk management for critical infrastructure is constructed. The results from reviewing the literature were used to identify problems in the current risk management practice. The findings from the literature review were used to define issues of the existing risk management practice. Empirical studies were conducted to investigate risk management practice in organisations that provide critical services, and a mixed-methods approach was followed for triangulation purposes which give research data reliability and validity. The qualitative method selected to triangulate the data was informal meetings/interviews. A set of semi-structured interviews was conducted with stakeholders within the organisation to confirm the findings and explore the current state of cybersecurity, the top management's expectations, and risk management limitations. This stage provided the foundation for developing the i-CSRSM framework.

### **Stage 2- Development of the i-CSRSM framework**

This stage presents the concepts necessary for the proposed i-CSRSM framework. We integrate the generic risk management concepts such as threat and vulnerability with CTI concepts such as TTP and indicators to improve and efficient risk management practice. In i-CSRSM framework development, risk assessment is considered to evaluate risk factors, considering the adequacy of existing controls and deciding whether or not the risk is acceptable. It is essential to measure the magnitude of the impact of a risk factor on critical infrastructure. The i-CSRSM concepts and their unique properties that are important for extracting features are then fed into the classifiers for risk prediction. Once the risk factors have been identified, the different controls regarding the organisation's security are introduced to mitigate those risks. ML is used to evaluate the effectiveness of the existing controls and recommend more controls.

### **Stage 3- Evaluation of the Case Study**

This stage introduced the proposed framework to organisations stakeholders, explained how it improves the risk management process and uses theory and decision-making techniques to conclude risk assessment results. A case study was conducted to evaluate the i-CSRSM framework in a natural cyber environment. The case study began with an entrance meeting between the stakeholders and the researcher to set the organisations objective, scope, methodology and related risk management procedures. Information was gathered from relevant documents such as minutes of the meeting and Policies and Procedures Handbook and kept in the working paper file. A questionnaire was circulated to different information systems departments throughout the organisation, including system administrators, security experts, IT supervisors, and top management to assess the applicability of the framework.

### **Stage 4- Discussion on the usability of the i-CSRSM framework**

After completing the case study, the practicality and usability of the i-CSRSM framework to enhance overall cybersecurity in organisations was judged. The framework's practicality and usability were

used to determine the framework's validity and applicability, its process, and i-CSRMT in supporting real-world organisations to achieve risk management. Figure 3.2 illustrates the analysis design method utilised in this study, which consists of four essential steps.

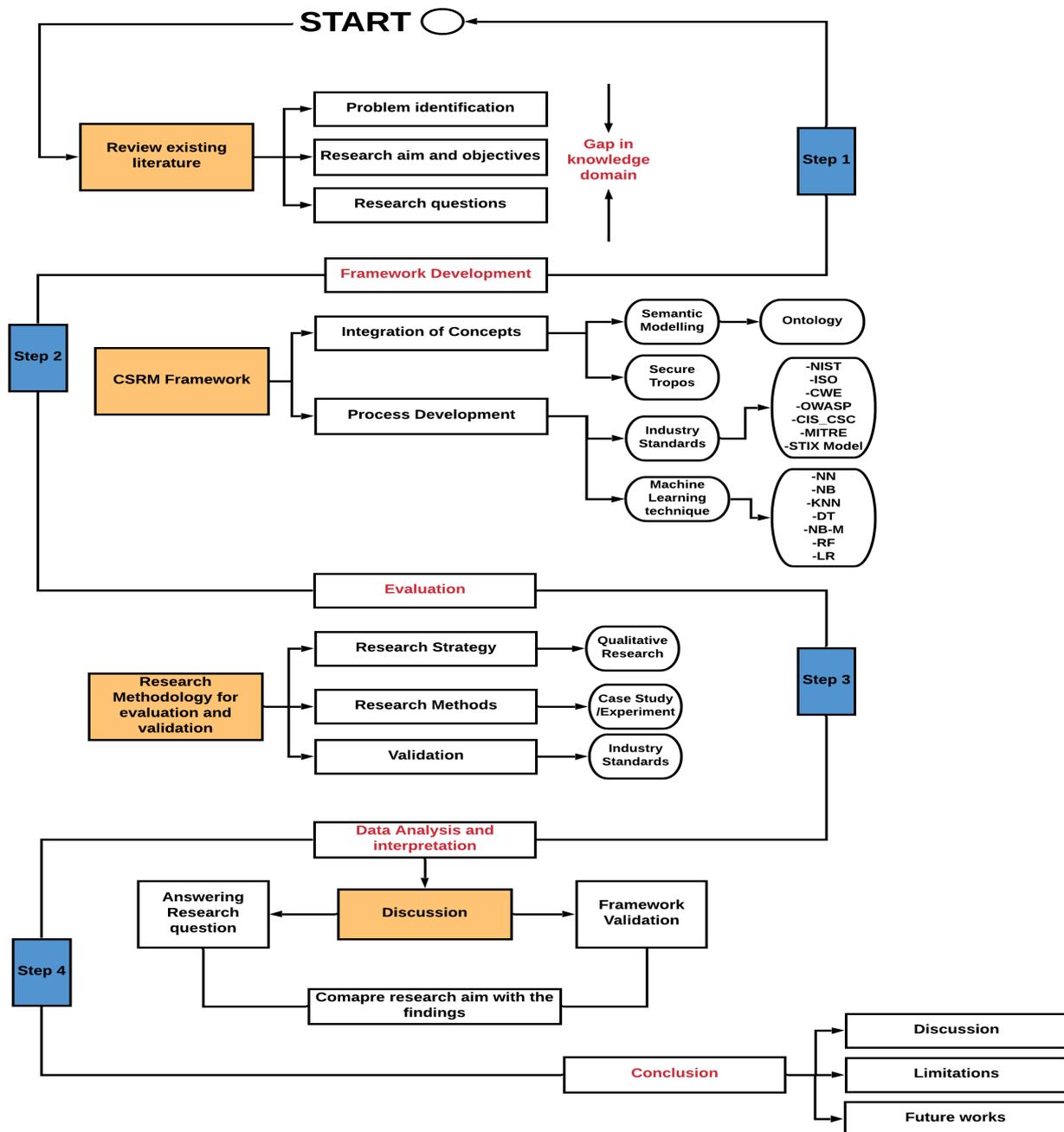


Figure 3.2: Summary of Research Design

### 3.5. Research Strategy

The study approach outlines procedures for determining suitable research methods for analysing, testing, and validating the research hypothesis (Coffey and Atkinson, 1996). (Lewis, 2015) discusses

that such study approaches are ideally adapted to specific research background and how the preferred approach will answer research concerns. Research methodology, research, architecture, data collection techniques, data interpretation, and evaluation are all components of a research approach. (Creswell and Creswell, 2017) describe a research strategy as arbitrary because the strategy is chosen based on the research challenge's characteristics. According to (Oates, 2005), there are only five research methods in social research: interview, case study, experiment, narratives, and archival material analysis. According to (Denscombe, 2008), there are only four analysis strategies: case analysis, survey, historical review, and experimental study. The research approach chosen is subjective and is determined by the essence of the research challenge. According to (Mills, 2000), there are four primary analysis strategies: case analysis, action testing, laboratory, and survey. When a technology is implemented into an enterprise, action analysis is typically performed to analyse and clarify the technology's socio-technical impact on customers and operations. Action analysis has been commonly used as a technique in information system research since it seeks to respond to both people's realistic needs and the socio-technical model's priorities. As a consequence, action analysis with case study and tests was selected for this review.

### **3.6. Action Research**

This research used a participatory action research (PAR) methodology to implement and evaluate the proposed framework. According to (Brydon-Miller, Greenwood and Maguire, 2003), intervention analysis is supposed to be implemented in real-life challenges rather than laboratory experiments. Action study takes a systematic approach to problem-solving by integrating various data collection and interpretation approaches and tools (Baskerville and Wood-Harper, 1996). The primary distinction between action analysis and other research approaches is the participant's active involvement in the research, undermining objectivist science, which contends that the researcher should be an unbiased observer (Kemmis, McTaggart and Nixon, 2013). Therefore, the rationale behind adopting the PAR is the nature of this research that requires interpreting the qualitative approach's findings with reasoning rather than presenting quantitative data. Also, the action research provides high level of practical relevance to the subject being studied. Action research allows data to be gathered by employing various methods i.e. observation, experiment, interview and written cases. We have utilized the experiment and case study method to collect the data.

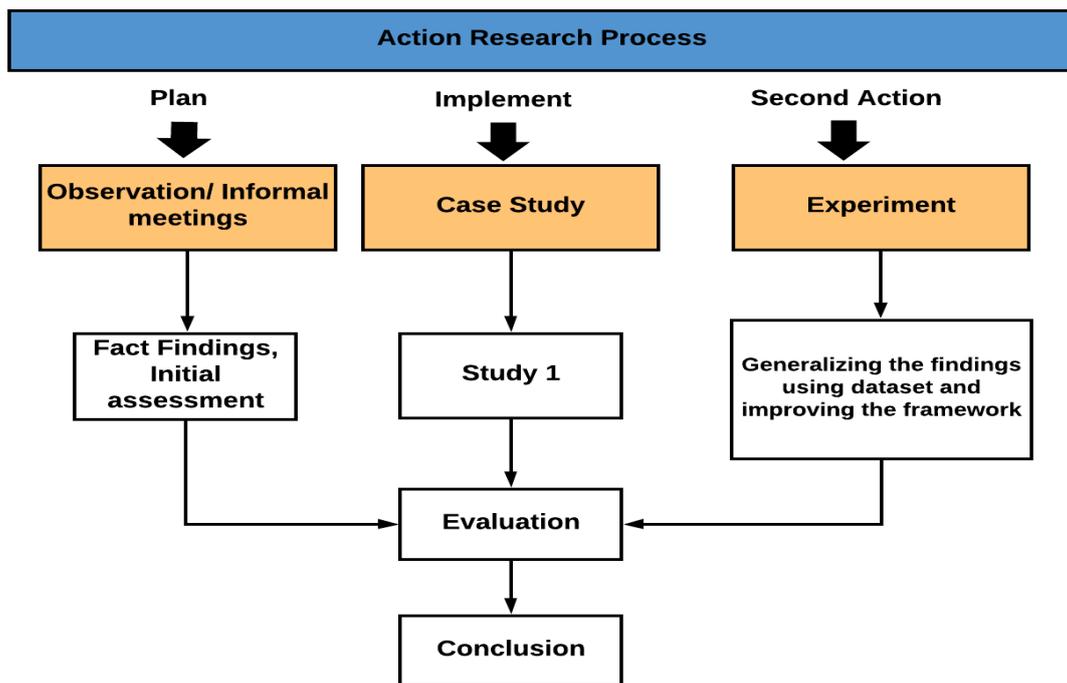


Figure 3.3: Evaluation process of the proposed framework

### 3.6.1. Case Study

A case study method is selected for this research. A case study is defined as a strategy to focus on understanding the dynamics present within single settings (Eisenhardt, 1989). When conducting a case study, the following process is involved (Runeson and Höst, 2009); case study design, data collection and analysing data. Therefore, an empirical evaluation was carried out through a case study to validate the framework's applicability and to demonstrate the validity of the i-CSR framework. The experiment is also carried out on a dataset to further explore the validity and usefulness of using ML techniques as part of the i-CSR framework, enabling the researcher to establish findings.

### 3.6.2. Data collection methods

Data collection from the case study is an essential process, and one of the most effective methods for finding all relevant information for this study (Cassell and Symon, 2004). Data collection and interpretation play an essential role in advancing the research hypothesis. According to (Yin, 2009), there are six essential data collection techniques to use in a case study setting, including informal sessions, conferences, focus group discussions, direct evaluation, reporting, tangible objects, and participant observation. In the course of the case study context implementation, different data collection techniques have been used. As it provides many potential data collection options, a case study is a flexible tool for stakeholders who want to understand specific problems in the workplace

(Turner and Danks, 2014). Also, both informal and formal data collection methods, such as interviews and questionnaires, were used.

The initial step for data collection is through documentation made during the framework implementation process, and informal meetings, observations, workshops, and interview have been used throughout the implementation process. The data collection process started with understanding the system context and interviewing the selected staff. We also reviewed various organisational documents to understand the existing policies and practices relating to risk management and information security. Note that we provided an overview of the integrated risk management approach before starting any data collection. The collected data were analysed by following both qualitatively and quantitatively methods. The analysis unit considered the existing risk management process, the number of identified risks and the effectiveness of risk control. Finally, we have taken the participants' view relating to the integrated risk management approach.

### **3.6.3. Interviews**

The primary data techniques used in this research were interviews, group discussion and participant observation. Interviews were conducted to evaluate the implementation process of an i-CSR framework based on a combination of subjective and objective questions. In qualitative research, there are two types of interviews; structured and semi-structured interview. A structured interview is rigid as the interviewer reads from a script, and findings are generally straightforward. Unstructured interviews tend to be very similar to informal conversation as the interviewers do not know all the necessary questions. In this research, triangulated semi-structured interviews were performed. Interviews were conducted during the initial step to investigate the existing risk management practice and later evaluate the i-CSR framework.

### **3.6.4. Informal Meetings/Workshops**

To gain feedback on the implementation process, informal meetings were held. This serves as an introduction to the process for all stakeholders and guidance in the implementation process.

### **3.6.5. Observation**

In this research, observations were conducted to investigate how a specific task is carried out. This approach is used to closely monitor and observe how well the stakeholders applied the framework. Observations were recorded and analysed on how the i-CSR framework is performing.

### **3.6.7. Documentation**

In this research, document analysis was used to obtain preliminary and background information about the case study and dataset to understand the scope of the processes and portfolio.

### **3.6.8. Experiments**

In this research, experiments have been carried out by the researcher to observe and test the effect of ML techniques in predicting risk types using a dataset.

### **3.6.9 Analyse Data**

The information gathered is analysed using both qualitative and quantitative techniques. It is essential to evaluate data to identify relationships between the group, person, program, or process identified in the problem statement. These relationships should address the research questions. Analysing data between cases followed by cross-checking data between cases is important (Eisenhardt, 1989). Once each case has been analysed, related themes between cases can be identified. According to (Turner and Danks, 2014), there are two types of analysis in a case study research; structural analysis and reflective analysis. The structural analysis focuses on identifying patterns, while reflective analysis uses the researcher's judgement to gather conclusions. This research applies reflective analysis, which means it uses all relevant evidence, explores in detail all interpretation, and addresses the most significant aspect of i-CSR framework for critical infrastructure.

### **3.6.10. Expert Opinion**

Expert opinion is commonly used to determine a product is possible strengths and weaknesses before it is rendered accessible to consumers (Hasson, Keeney and McKenna, 2000). Expert opinion was used to generalise the case study results and gather opinion on the suggested framework's usability in the critical infrastructure domain. It has also been used to validate the dataset's mapping. The researcher has compiled several possible domain experts. Although the study covers a wide range of topics, including technical, organisational, and consumer viewpoints, specialists from many of these fields were chosen. The researcher weighed the amount of time the expert has worked on the topic, commitment to experience, position in the subject, professional qualification or another accomplishment in the subject domain, and their area of interest when choosing the expert. The framework's functionality, accessibility, and tasks were clarified to the participants in a user manual context.

## **3.7. Integrated Cybersecurity Risk Management (i-CSR) Framework**

An overview of the i-CSR framework is presented in this section. The framework can be defined as the set of ideas or basic conceptual structures used for dealing with a particular problem (Shackel, 2009). According to (Johnson and Foote, 1988), a framework represents a collection of concepts that an abstract architecture for solving a problem is reflected. The structure generally means a collection of definitions that main coordinate factors, structures, or constructs, as well as their relationships (Zachman, 1987). Frameworks are utilised in various fields, including enterprise processes, product

development, and information management. To ensure the rigorous application of philosophical theories, this analysis used a framework-oriented methodology. It also aids in the identification and interconnection of conceptual elements to ensure performance, efficacy, and accuracy and the identification of interrelationships between them. Therefore, the i-CSRSM framework introduced a logical representation of the interrelated key concepts needed for implementing a conceptual remedy.

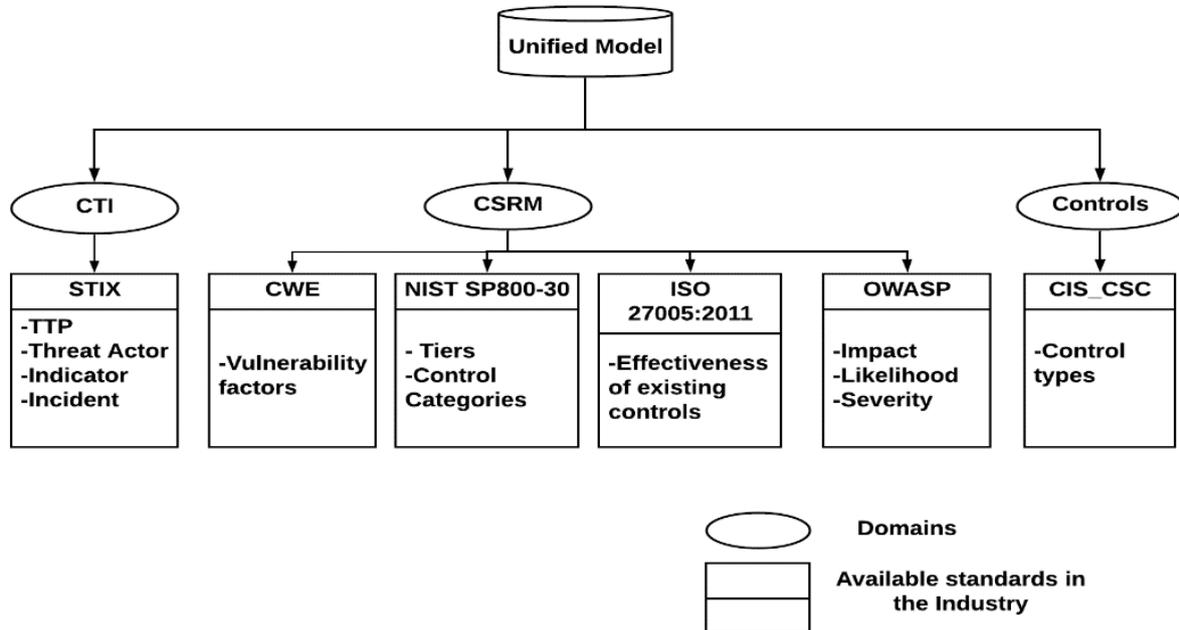
Furthermore, the i-CSRSM framework integrates several concepts that act as a common language for enhancing risk management and providing a comprehensive means for managing cybersecurity risks. It decomposes and associates a high-level collection of concepts with one another to include a level of clarity that makes for precise implementation.

### **3.8. Approach to Framework Development: Unified approach**

We considered four main areas for the unified approach. They include; CTI, existing risk management standards, controls and machine learning techniques. These four domains are integrated to form a unified approach used to improve risk management in critical infrastructure. Understanding threats and managing, monitoring, and communicating the presence of risks in critical infrastructure is the aim of the unified approach for the i-CSRSM framework. As a result, the unified approach builds on existing industry practices to help organisations achieve overall risk control by ensuring that all steps and activities are carried out following universally agreed security criteria. For example, CIS CSC (Mbanaso, Abrahams and Apene, 2019) defines controls and assesses the efficacy of current controls using some of the parameters mentioned in (Dittmeier and Casati, 2014). The STIX model (Barnum, 2012) for identifying CTI, i.e. threat actor attack pattern and information, CWE for communicating the impacts of vulnerabilities, OWASP provides basic techniques to protect against web application security challenges, and risk management standards such as NIST SP800-30 and ISO 27005:2011 (Martin, 2007) for understanding risks in critical infrastructure. The proposed approach integrates the use of fuzzy set theory for determining and ranking critical assets and integrates CSRSM concepts such as threat actor, assets, TTP and controls, extracts features from these concepts so that ML classifiers can predict certain risk types. The rationale for choosing these methods is that they are widely accepted standards for raising security awareness by identifying some of the most severe cyber-physical organisations' faces.

Note that, even though the unified approach uses these approaches, our contribution is beyond these existing works and focuses on improving risk management practice using CTI information. Our approach supports analysing risks by considering the attacker's profile and the evolving threat landscape. This makes our work different from STIX, emphasising analysing the threat profile and sharing this information. On the other hand, our work integrates CTI to provide a clear and vital role in risk management by identifying, assessing, and tracking threat, as well as evaluating current vulnerabilities in light of such threats. Integrating CTI with CSRSM helps the organisation to analyse

and determine the likelihood and impact of risk. Figure 3.4 shows several areas that incorporate into a unified approach.



**Figure 3.4:** Unified approach model for the development of i-CSR

### 3.9. Conceptual View of i-CSR

The conceptual approach generally requires a straightforward understanding and precise reinterpretation of abstract ideas or principles to understand what a system, frameworks, or concepts are, what they do, how they achieve clear objectives, and how they can be implemented (Chen, 1976). Conceptual view accurately and precisely provides a meaning for the concepts and models the concepts such that anyone with no knowledge will understand what risk management means. It also serves as the conceptual foundation used to develop the i-CSR framework for critical infrastructure protection.

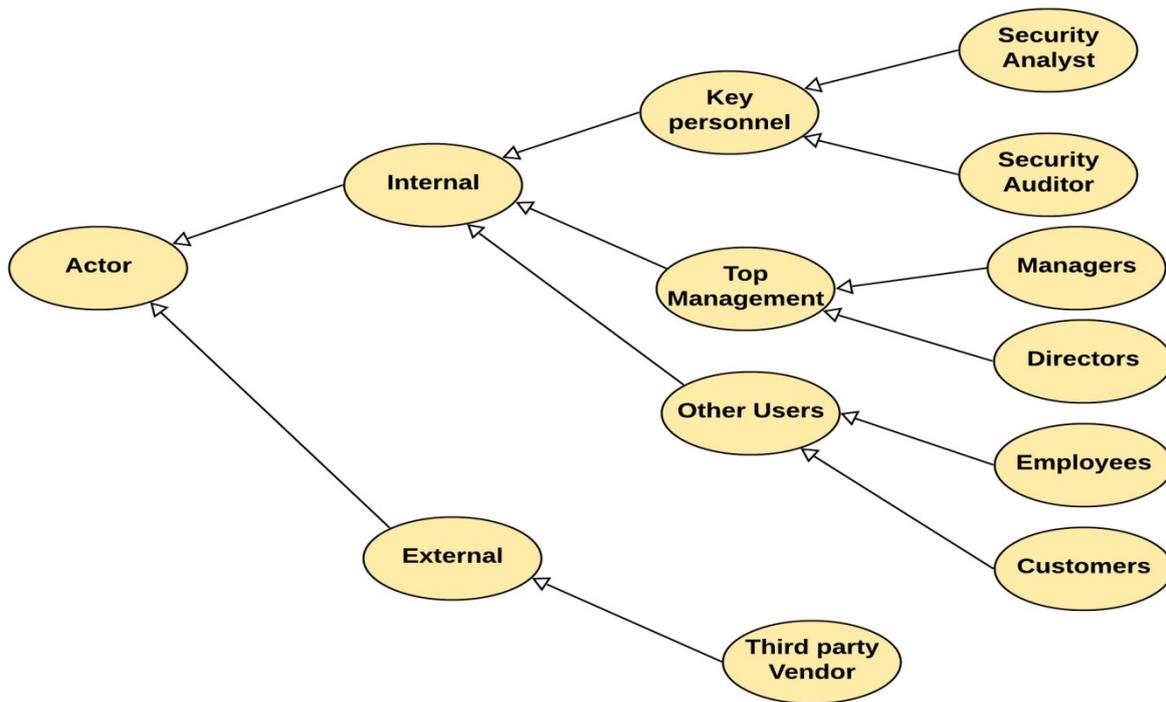
Adopting a common terminology for the concepts would help interpret the concepts and the overall process implementation. For defining and explaining concepts in detail, conceptual modelling is highly recommended. These concepts are linked to vulnerability assessment, threat identification, risk management, and evaluating the effectiveness of existing controls. The emphasis is on the visual representation of the concepts to help their evaluation and study, utilising logical representation for each concept. Graph visualisation is one method that may be used to understand the structure of each concept further. Therefore, we used Protégé for graphically visualising the concepts and it includes a concept editor and other visualisation extensions. One of the most widely used ontology editors is

Protégé, is free, open-source ontology editor developed at Stanford University (Noy and McGuinness, 2001). The i-CSRSM framework concepts are organised in a generalisation hierarchy using Protégé using "is-a" links (inheritance). Each conception is made up of zero or more sub-concepts. To explain the modelled concepts' different features, each definition has an entity (relationship) and data (characteristics) properties. The following are the identified concepts and their ontological representations:

### **3.9.1. Actor**

An actor represents an individual, such as an organisation or a human user, that has a strategic goal within its organisational context and performs specific activities (Castro, Kolp and Mylopoulos, 2002). In other words, actors could be an organisation, functional department or set of people involved in providing, requesting or receiving critical services through many forms of information exchange. Actors are related and interact with each other in one or another. An organisation can be an actor with many different actors, such as staff and clients that use the services provided by the organisation. The interaction between actors is established by factors such as delivery and consumption of services, exchange of information or the provision of supporting computing needs. The increased service orientation and the opportunities of the critical services offered by the critical infrastructure's computing platforms have given rise to a set of new roles within the critical infrastructure. The listing of actors varies and will be determined in every organisation according to its volume of activities and resources.

The Actor is divided into an external and internal actor. The internal Actor is the critical infrastructure organisation that supplies infrastructure and other services needed to run its operations and has skilled personnel who play different roles such as risk manager, information technology security analyst, senior engineer. External actors are mainly users outside the organisation who make use of the services provided by the organisation. They are also third-party actors who provide various forms of computing services such as internet services and are responsible for delivering multiple other services. The listing of actors varies and will be determined in every organisation according to its volume of activities and resources. There are different types of actors, and each has a role. It consists of sub-classes such as external and internal, as shown in Figure 3.5.



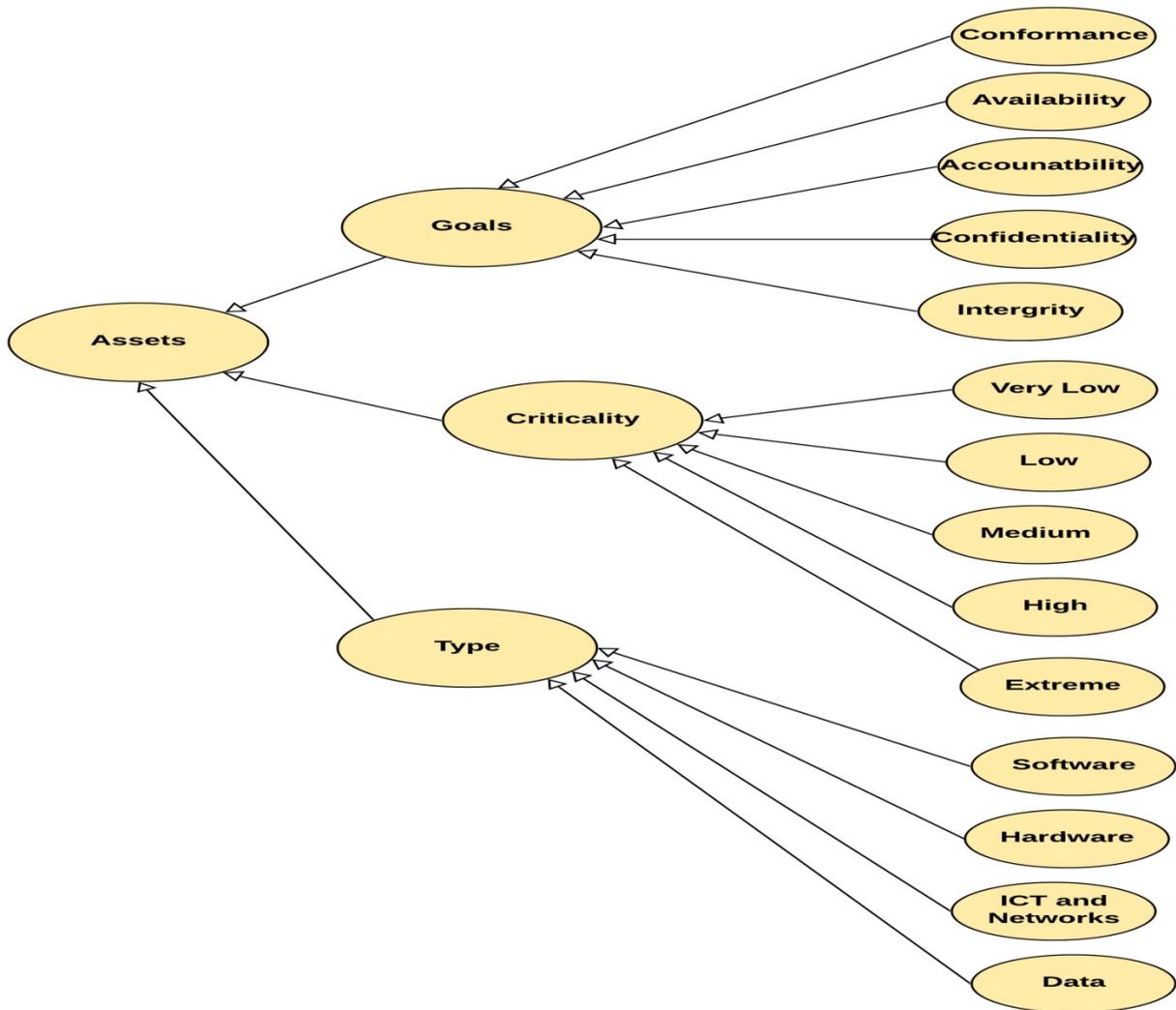
**Figure 3.5:** Actors Classification concept for the development of i-CSRM process

### 3.9.2. Assets

Assets are necessary and have values to the organisation, such as an organisation's application or software. The critical assets are required for the stable and reliable functioning of the organisations business functions. This concept involves identifying an organisation's asset in terms of the assets used within the organisation. Assets are profiled to include categorisation according to asset criticality, asset security goal and supported business function to the organisation. The relevance of asset profiling is to help the organisation to have a standard, consistent, and clear understanding of asset boundaries, clearly designated asset goals, a description of how the asset is stored or processed, and an opportunity to determine the asset's criticality. The asset concept consists of sub-classes such as *asset types*, *criticality* and *asset goal*, as shown in Figure 3.6:

- **Asset profile:** It describes the necessary descriptive information about the many components of all the organisation's asset types. Assets are profiled in a register to give a clear understanding of all assets and their subcomponents. The asset categories include:
  - Data are information stored and used by a computer system
  - Software is a program or application used by an organisation for its business activities. If such assets are not managed properly, they may result in financial loss, reputational damage and violation of privacy
  - Hardware is the collection of physical components of a computer system

- Information communications and networks are the physical connection between networked computing devices using cable media or wireless media.
- **Asset security goals:** Each asset aims to achieve a security goal to determine the impact that may result from unauthorised access. Asset goals are established using five key areas related to information assets, including *confidentiality*, *integrity*, *Availability*, *accountability*, and *conformance*.
- **Asset criticality:** Criticality is the significant indicator used by organisations to determine which asset is of more value to the organisation. The security goals are used to measure the criticality level of each asset within the organisation. An asset type's criticality level can be from highly critical, moderately critical, to low critical. Assets are highly critical if they are the most valuable to the organisation; a moderately critical rating represents a moderate value; while low criticality means little or no value.
- **Supported Business Process:** business processes are structured activities or tasks backed by assets to serve a particular business objective or produce a service or product. Each asset is related to the specific business function that it supports.



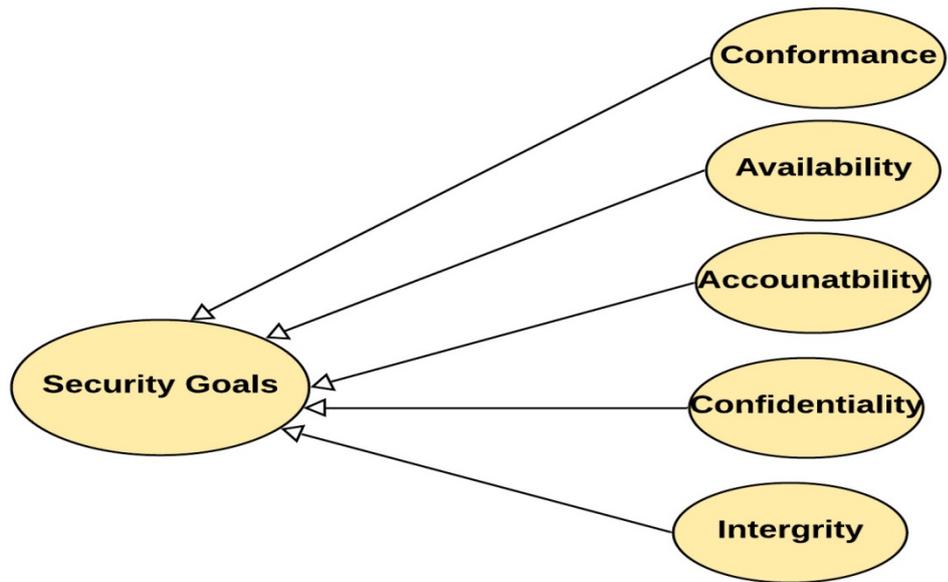
**Figure 3.6:** Asset Classification concept for the development of i-CSR process

### 3.9.3. Goals

The goal of any critical infrastructure includes; the concealment of sensitive data against unauthorised users, ensuring the organisation's assets are made available and accessible to the end-users, and the assets' ability to perform their required functions effectively and efficiently without any disruption or loss of service. Therefore, this concept identifies each asset's goals in terms of security and organisational context, and the security analyst carries it out. Identifying security goals is an essential consideration for an organisation to determine what fundamental security principles must be ensured for assets to be accessed or modified during storage, processing or transmission by authorised systems, applications or individuals. The assets' goals represent factors against which asset criticality is measured; they are used to distinguish those assets whose loss could significantly impact the organisation's objectives. They include:

- *Availability (A)*: Availability refers to ensuring that an asset is made available and accessible to authorised users when and where they need it. This asset goal is essential, and one of the primary objectives to ensure the organisation's reliable operation. In the case the asset gets interrupted, it must be recovered and continue secure operations without noticeable effects.
- *Integrity (I)*: Asset integrity refers to an asset's ability to perform its required functions effectively and efficiently without any disruption or loss of its services. The modification or destruction of an asset leads to the loss of the integrity of the asset. Loss of asset integrity may occur due to the intrusion in the cyber domain by the attacker or disgruntled employees or by human error, which degrades the asset's reliability.
- *Confidentiality (C)*: Asset confidentiality refers to assets staying secured and trusted and preventing unauthorised disclosure of sensitive data. Exposure to a sensitive asset can lead to a loss of confidentiality. Confidentiality ensures that only those with predefined rights and privileges to access an asset can do so. One of the simplest methods to provide confidentiality is to install encryption/decryption components at both ends of an unsecured connection (Taylor and Sharif, 2017).
- *Accountability (ACC)*: This asset goal requires that attack or incident actions that occur on an asset are tractable to the responsible system or Actor. It must be ensured that an authorised actor or an attacker who acts cannot deny involvement.
- *Conformance (CON)*: This asset goal ensures that the assets such as services meet the specified standard. Assets must operate as intended without variation to expected behaviour, functions and regulatory requirements. The asset must be secured from vulnerabilities that can be exploited to cause unwanted behaviour. Any breach or deviation from specified action constitutes non-conformance.

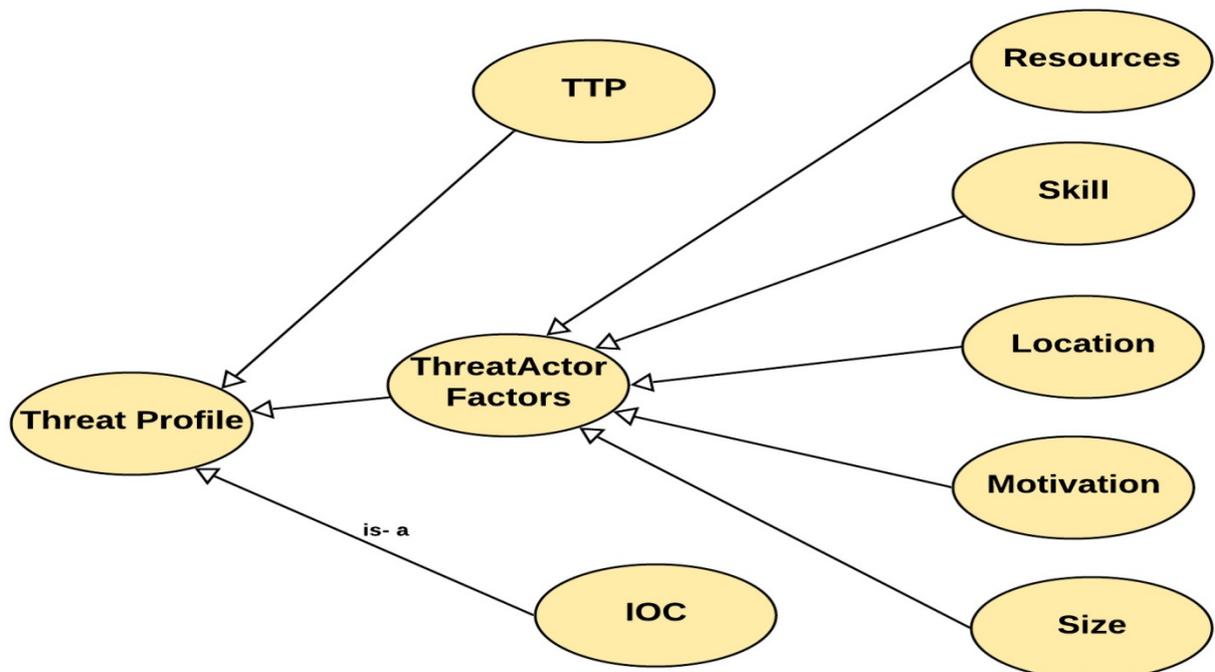
The control concept consisting of sub-classes such as *Availability, integrity, conformance, confidentiality and accountability, as shown in Figure 3.7.*



**Figure 3.7:** Goal Classification concept for the development of i-CSR process

### 3.9.4. Threat Actor

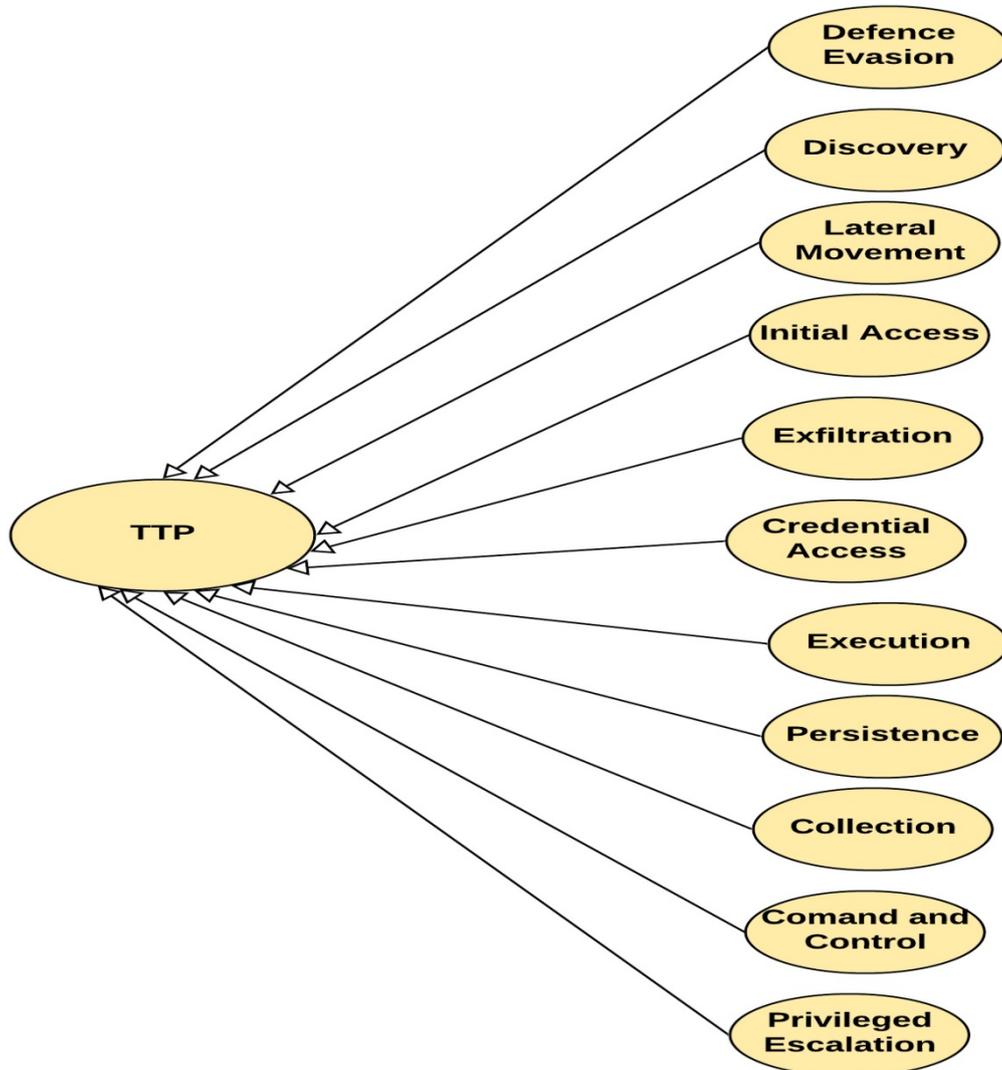
Threat actors are actors with malicious intents to execute a cyber-attack. This concept aims to allow identification and characterisation of the threat actor so that organisations can understand the attack, its trend, and the factors to determine the risk level. It consists of sub-classes like *Skill*, *Motivation*, *Location*, *Resources*, *Size*, and *Opportunity*, as shown in Figure 3.8.



**Figure 3.8:** Threat Actor Classification concept for the development of i-CSR process

### 3.9.5. Tactic, Techniques and Procedure (TTP)

This concept describes various methods in which a threat actor executes an attack and possible outcome. TTP involves the pattern of activities or methods associated with a specific threat actor and consist of the threat actor's specific behaviour (attack pattern) and specific software tools that can be used to perform an attack. A threat actor uses TTP to plan and manage an attack by following a specific technique and procedure. Therefore, TTP from the STIX model categorises attacks into the eleven tactics and the different techniques under each tactic provided by MITRE (Strom *et al.*, 2017). TTP consist of sub-classes such as *initial access*, *execution*, *persistence*, *privileged escalation*, *defence evasion*, *credential access*, *discovery*, *lateral movement*, *collection*, *exfiltration* and *command and control*. These subclasses further consist of their subclasses, as shown in Figure 3.9. For example, *initial access* consists of subclasses such as *Spearphishing attachment*, *Spearphishing link*.

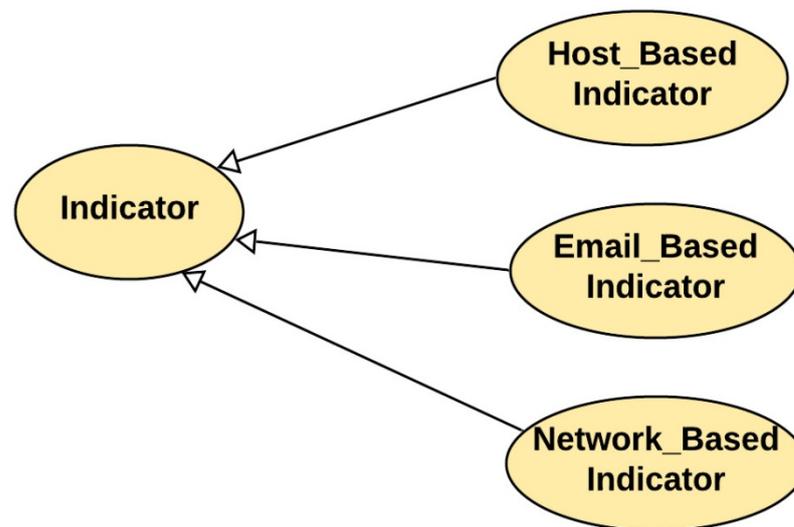


**Figure 3.9:** TTP classification concept for the development of i-CSR process

### 3.9.6. Indicator of Compromise

The indicator concept contains a pattern that can be used to detect suspicious or malicious cyber activity. IOC is detective in nature and is for specifying conditions that may exist to indicate the presence of a threat along with relevant contextual information. Organisations should be aware of the data associated with cyber-attacks, known as indicators of compromise (IOC). IOC is commonly partitioned into three distinct sub-classes (Tounsi and Rais, 2018). The sub-classes include *network indicator*, *host-based indicator* and *email indicator*. These sub-classes have their sub-classes, as shown in Figure 3.10. For instance, the *email indicator* has a sub-class *email attachment*, *email link*. The *network indicator* has a sub-class *IP address*.

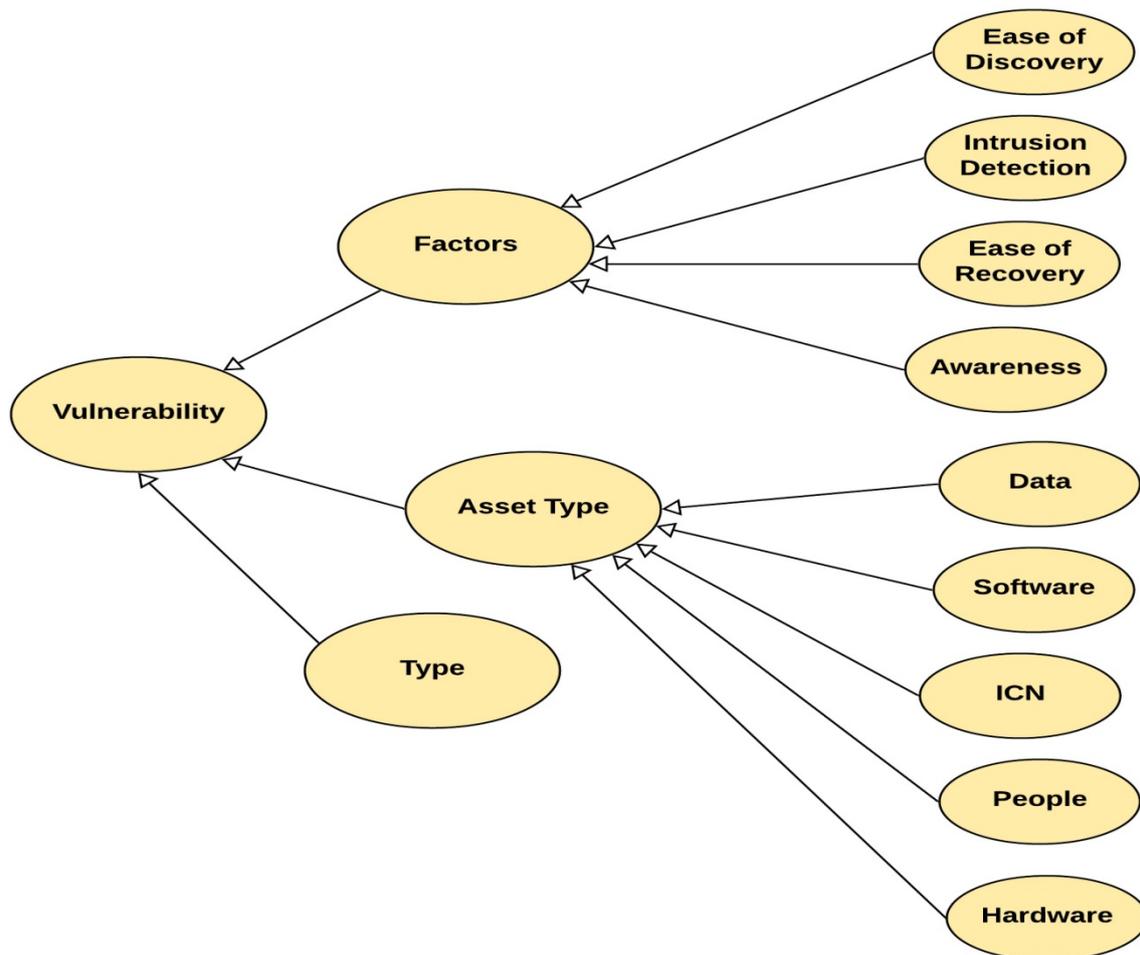
- *Network indicators* are found in URL and domain names used for command and control and link-based malware delivery. They could be IP addresses used in detecting attacks from botnets, known compromised servers and systems conducting DDoS attack.
- *Host-based indicators* are found by analysing infected computers. They include malware names and decoy documents or file hashes of the malware being investigated. Dynamic-link libraries (DLLs) are often targeted, and registry keys could be added by malicious code to allow for persistence.
- *Email indicators* are created when threat actors use free email services to send social engineering emails to target organisations. The email source address and subject are created from addresses that appear to be recognisable individuals or create intriguing subject lines. Attachments and links are also used for deceiving individuals.



**Figure 3.10:** Indicators of Compromise Classification concept for the development of i-CSR process

### 3.9.7. Vulnerability

Vulnerability is the weakness or mistake in an organisation's security program, software, systems, networks, or configurations targeted and exploited by a threat actor to gain unauthorised access to an asset (system or network) using TTP. There are several ways an attacker can exploit vulnerabilities in critical infrastructures, thereby causing severe damage. This could be from a threat actor only being able to view information and to a worst-case scenario. Regardless of the Vulnerability discovered, the threat actor could have little or complete control over the system and any action taken is referred to as a cyber-attack. It consists of sub-classes such as *Vulnerability types*, *Vulnerability Factors*, *Assets targeted*, as shown in Figure 3.11.

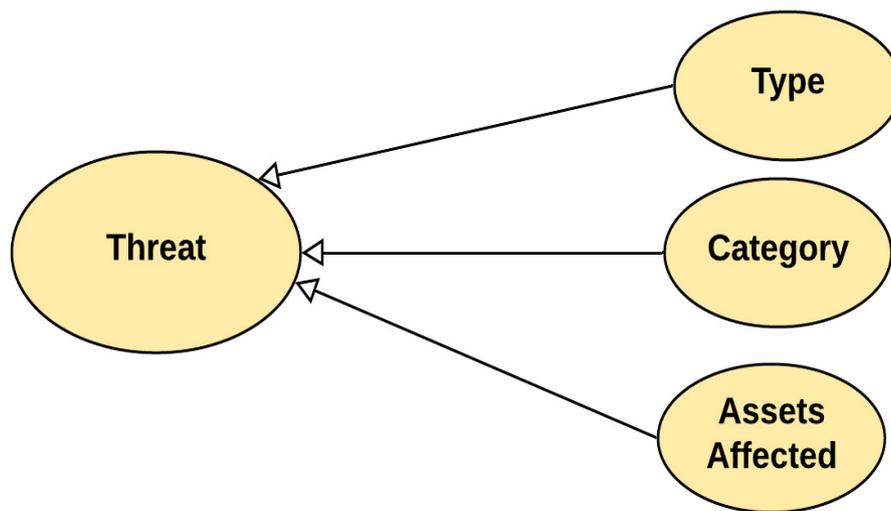


**Figure 3.11:** Vulnerability Classification concept for the development of i-CSR process

### 3.9.8. Threat

The threat is the possibility of a malicious attempt to damage or disrupt an organisations asset (systems or networks), access files and infiltrate or steal data. The threat is identified as an individual or group of people attempting to gain access or exploit a vulnerability of an organisation's asset or the

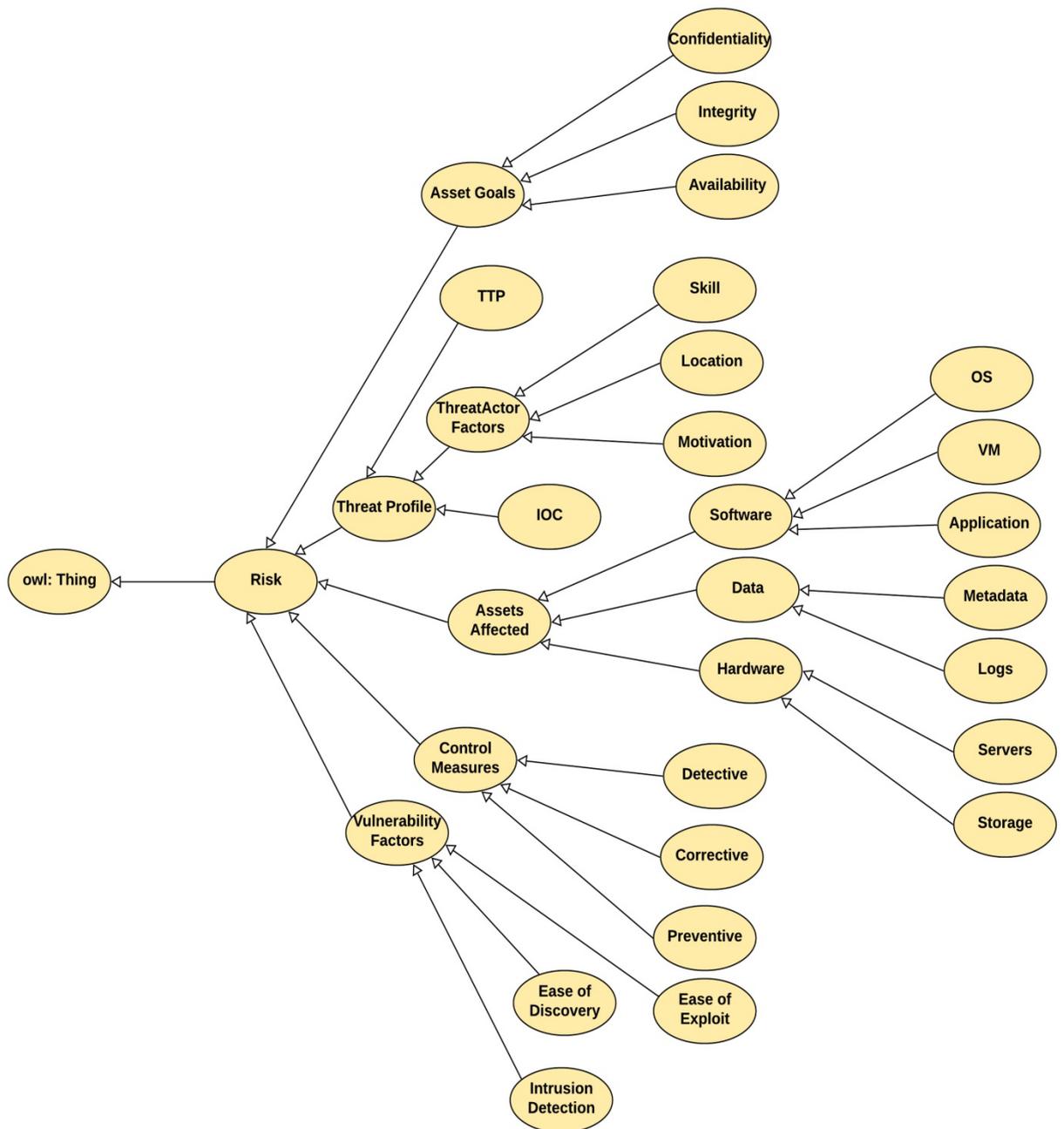
damage caused to hinder the organisations' ability to provide its services. Threats such as denial of service or malware attacks are famous threats to critical infrastructures, causing security challenges to the interconnected devices (Baldoni, 2014). Threat profile allows for the identification and understanding of threat characteristics. Therefore, organisations need to categorise each threat according to their goals and purpose and the assets targeted. By classifying these threats, the stakeholders check the category that a threat falls under and the most common assets affected by a particular threat. With this, a solid foundation of threat information sources is made available. It consists of sub-classes such as *Threat types*, as shown in Figure 3.12.



**Figure 3.12:** Threat Classification concept for the development of i-CSR process

### 3.9.9. Risk

Risk is defined as the probable failure of an actor (organisation or individual) to fulfil its goals, such as confidentiality, due to the probability of a threat actor obstructing the Actor's goal. Organisations cannot wholly avoid Risk; however, it is the actors' role to ensure that risks are kept to a minimum level to achieve their goals. Therefore, organisations need to identify security risks that need to be rated. The consequence of Risk resulting from cyber-attack can lead to financial loss, reputational damage, privacy violation and non-compliance consequences, leaving users distrustful of services. To understand a cyber-attack, we have to study the nature of the attack and its motivation (Gandhi *et al.*, 2011). Therefore, for risk severity to be estimated, it is essential for information about the threat actor, vulnerability factors and the impact of a successful exploit affecting the security goals of the assets to be gathered. The following sub-classes are involved in identifying the risk level; *threat type*, *vulnerability type*, *risk type*, *control type*, *Security Assets goal* as shown in Figure 3.13.

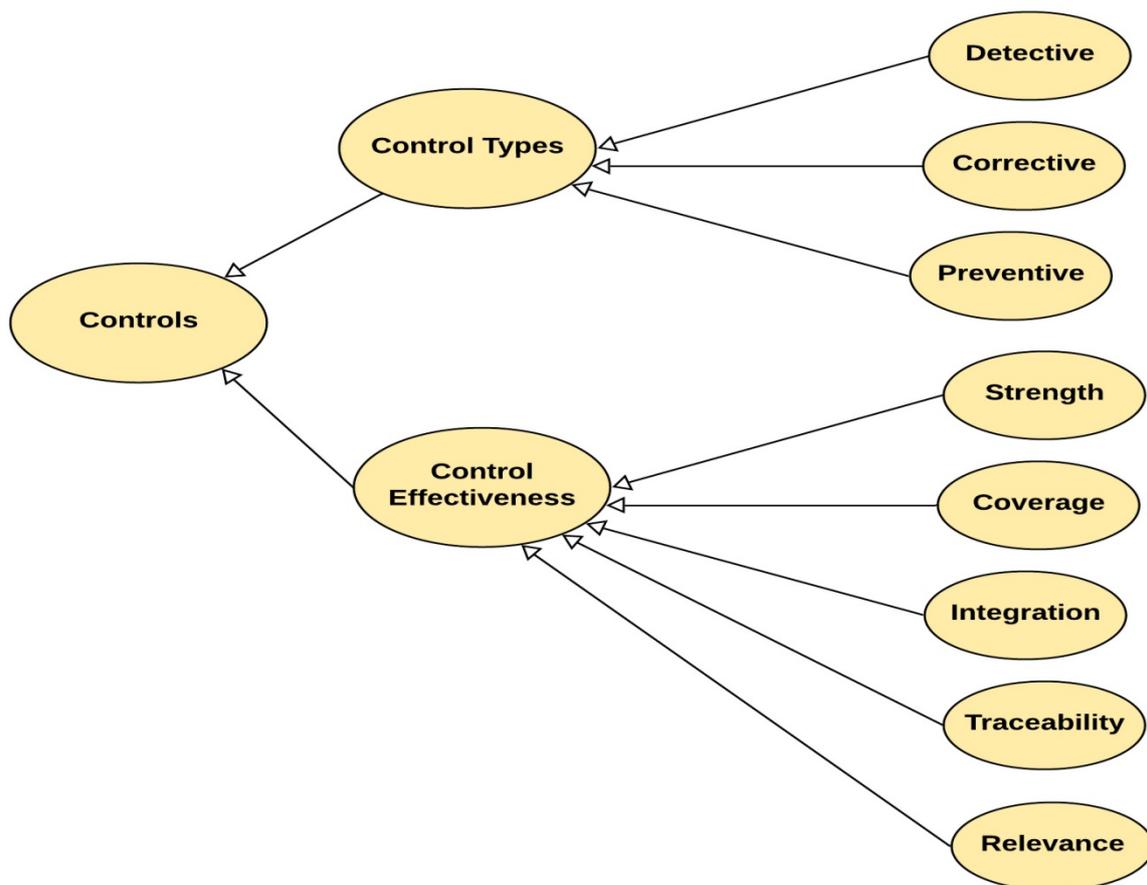


**Figure 3.13:** Risk Classification concept for the development of i-CSR process

### 3.9.10. Controls

These are the corrective, detective and preventive actions to mitigate Risk. Preventive controls keep errors or irregularities from occurring; detective controls detect errors and irregularities, which have already occurred and ensured their immediate correction. Corrective controls help to mitigate damage once a risk has materialised. This means that the level of attack determines the type of control used, and the effectiveness of the existing controls is evaluated. The CIS\_CSC recommended a list of controls that we adopt for the proposed framework. This means that the level of attack determines the

type of control to be used and the effectiveness of the existing controls. To evaluate the effectiveness of the existing controls, an assessment of each control objective is carried out. We apply a set of criteria: Relevance- The level to which the control addresses the relevant control objectives under analysis. Strength- The strength of the control is determined by a series of factors. Coverage is the levels at which all significant risks are addressed. Integration- The degree and manner in which the control reinforces other control processes for the same objective—traceability- How traceable the control is, which allows it to be verified subsequently in all respects. The sub-class is *control type* and *control effectiveness*, as shown in Figure 3.14.



**Figure 3.14:** Control Classification concept for the development of i-CSR process



The Meta-model, illustrated in Figure 3.14 shows the relationship between the concepts. An actor represents an entity, an organisation or a human user that generates strategic, operational and tactical plans within its organisational setting. Identifying actors is essential for determining the roles played by actors and the implementation of the framework's process. An actor owns a wide range of assets that require several security goals for supporting the business process. As a result, critical assets to operations are comprehensively profiled to include the security goal every asset must achieve, the business process supported by assets, and, importantly, each asset's criticality to the organisation. The Actor is represented as having an interest in the organisation's assets. These assets have security goals such as confidentiality, integrity and Availability for the business's continuation and reputation, and the attainment of one or more of the goals is always their focus. The Actor has complete control over its assets and needs to keep the assets secure for its continuity, but these assets are prone to weaknesses in their systems, known as vulnerabilities. Vulnerability is the weakness or mistake in an organisation's security program, software, systems, networks, or configurations targeted and exploited by a threat actor to gain unauthorised access to an asset (system or network) using TTP. When not addressed on time, these vulnerabilities can lead to a threat that introduces Risk, and this Risk is likely to lead to the exploitation of the assets. Risk is the failure of an organisation or individual to achieve its goals due to the malicious attempt to disrupt its critical services by a threat. Organisations cannot wholly avoid Risk; however, it is the actors' role to ensure that risks are kept to a minimum level to achieve the goals by integrating CTI to improve i-CSR. Therefore, the different controls regarding security and the organisation are introduced to help mitigate the risks.

The threat actor is a type of Actor with malicious intent characterised by their identity, suspected motivation, goals, skills, resources available for them to carry out a successful attack, past activities, TTP used to generate a cyber-attack and their location within the organisation's network. They try to impersonate actors by deceiving users of the critical infrastructure into believing them and then getting hold of some sensitive information or directly compromising their critical assets and leading to a significant risk to the organisation. This is done when vulnerabilities in an asset of the organisation are exploited using some TTP. A threat actor uses TTP to plan and manage an attack by following a specific technique and procedure. They involve the pattern of activities or methods associated with a specific threat actor and consist of the threat actor's specific behaviour (attack pattern) and specific software tools that threat actors can use to perform an attack leaving behind the attack's incident. The incident is the type of event that represents information about an attack on the organisation. Some specific components determine the type of incident, such as; threat types, threat actor's skill, capability and location, assets affected, parties involved, and time. With a specific attack pattern, the organisation tends to think broadly by developing a range of possible outcomes to increase their readiness for a range of possibilities in the

future. Indicators contain a pattern that can be used to detect suspicious or malicious cyber activity. They are detectives for specifying conditions that may exist to indicate the presence of cyber activity. An Indicator may be used to represent a set of malicious domains. They are a detective in nature and are for specifying conditions that may exist to indicate the presence of a TTP along with relevant contextual information. Indicators are not used to characterise any given threat actors behaviour, only how to detect it.

Table 3.1 shows the relationship between all the concepts.

**Table 3.1:** Relationship between Concepts

Source	Type	Target
Actor	Generates	Report
Actor	Needs	Assets
Threat actor	Impersonates	Actor
Threat actor	Exploits	Vulnerability
Threat actor	Uses	TTP
Threat actor	Generates	Incident
Threat actor	Attacks	Assets
Incident	Affects	Actor
Incident	Results to	Risk
Incident	Affects	Asset
Incident	Influenced by	Threat
Vulnerability	Influences	Threats
Controls	Addresses	Vulnerability
Control	Mitigates	TTP
Controls	Addresses	Threats
Controls	Mitigates	Incident
TTP	Exploits	Vulnerability
Indicator	Specifies	TTP
Indicator	Indicates	Threat actor
Indicator	Generates	Incident
Risk	Requires	Control
Risk	Affects	Actor
Risk	Requires	Control
Threat	Introduces	Risk

### 3.10. Summary

This chapter presented a detailed narration of the research methodology adopted in developing and evaluating the proposed framework. It outlined essential steps that have been taken, including; a

systematic literature review, framework development, process development, evaluation, discussion, and confirmation of research aims and objectives. It also presented the types of research approaches that exist and the chosen approach for this research. A research design provides an overview of the research structure, including methods used for data collection.

The research methodology used in developing and evaluating the proposed framework was described in depth in this chapter. It presented the main steps, such as a comprehensive literature review, process development, evaluation, discussion, and confirmation of research aims and objective. It also discussed the various research methods available and the methods chosen for this study.

This chapter also provides the fundamental properties and basics of i-CSR. It presented a new definition of security transparency from a cloud computing perspective and essential areas of focus for security transparency in the cloud. Also, it offered the reasons for ensuring security transparency and how transparency can support businesses. The chapter also discussed the salient properties of cloud security transparency such as auditability, accountability and assurance, as well as the barriers that hinder transparency. Further, the principles and categories of security transparency are introduced which provide the basis for developing the CSTF. Importantly, the chapter introduced security transparency deployment practices that are also used in determining the level of security transparency offered by CSPs.

## CHAPTER FOUR

### Process for the Integrated Cybersecurity Risk Management (i-CSRМ) Framework

#### 4.1. Introduction

This chapter presents an overview of the underlying process involved in the i-CSRМ framework. Primarily, the process aims to introduce different phases of activities that organisations can follow for understanding and managing risks by looking at essential considerations such as identifying roles, assessing critical assets, identifying vulnerabilities and threats, assessing risks, and evaluating controls. The process also helps organisations understand the associated risks and the necessary control measures to align with the business goals. The process helps organisations build a risk management profile from scratch to the end, meaning that they will provide accurate information about risks based on the context and validate whether expectations are being met by the organisation continuously. Therefore, the principal beneficiaries of the framework and its process are organisations that provide critical infrastructures responsible for ensuring the security of a given nation, its economy, and the public's health and safety and data protection. Hence, it is essential to emphasise that the framework does not focus on individual users who usually do not have as much obligation towards overall security, diverse requirements and responsibilities as organisations.

An essential aspect of the process is that it provides systematic activities for developing an efficient risk management approach that is mainly security-oriented and provides a roadmap for organisations to achieve overall cybersecurity. The process's core includes several diverse activities and steps to help guide key decision points about organisational context, threat and vulnerability activities, potential risks, and security controls. It helps identify and interlink risk management components for ensuring efficiency, effectiveness and consistency within different areas of the organisation.

Another essential feature of the process is that most of the activities are designed by considering various leading industry best practices, frameworks, guidelines, and standards applicable to all organisations regardless of their size or the domain in which they operate. This implies that the process is all-encompassing in nature and not tailored to a specific organisation type or solution but built upon high-level considerations to ensure important cybersecurity issues are not overlooked.

#### 4.2. Integrated Cybersecurity Risk Management (i-CSRМ) Process: A Unified Approach

The process for the i-CSRМ framework is simply a unified approach that leverages existing industry standards to assist critical infrastructures in attaining overall cybersecurity by ensuring that every step and

activity is performed according to generally accepted security principle. Sections of renowned industry standards, guidelines, frameworks and models were applied across different activities by looking at specific features within the standards and where they can be applied. Using this widely accepted standard is because they are industry standards and do not require any form of verification. The following are the different standards /guidelines:

#### **4.2.1. Cyber Threat Intelligence (CTI)**

For organisations to respond to their specific threats and make informed decisions on which countermeasures to deploy, they must have detailed threat information. Therefore, we consider STIX the most widely used CTI method for the specification, capture, characterisation and communication of standardised cyber threat information.

#### **4.2.2. Fuzzy logic**

For a successful risk management process, asset identification is crucial and needs to be initiated before any risk is identified. Therefore, we propose the use of fuzzy logic to determine the criticality of assets within an organisation. Our unified approach integrates the use of fuzzy set theory which provides a way of absorbing the uncertainty inherent to phenomena whose information is unclear and uses a strict mathematical framework to ensure precision and accuracy, as well as the flexibility to deal with both quantitative and qualitative variables (Zimmermann, 2011).

#### **4.2.3. Risk Management Standards**

We considered ISO 27005:2011 as a widely accepted risk management standard for our work. We also considered CWE for understanding the underlying weaknesses and OWASP methodology for determining the impact of risks.

- **Common Weakness Enumeration (CWE):** CWE seeks to understand and characterise vulnerabilities, misconfigurations or weaknesses that are likely to be targeted. It introduces a common weakness scoring system (CWSS), which provides a mechanism for prioritising software weaknesses consistently, flexibly, and openly. It is a standardised approach for characterising weaknesses and allowing organisations to make more informed decisions during the risk management phase and give higher risks (Martin, 2007).
- **ISO 27005:2011:** ISO 27005:2011 considers risk management as an integral part of the overall organisational processes, including evaluating the effectiveness of controls (Firoiu, 2015). We consider identifying the existing controls and their effectiveness by following this standard.
- **OWASP:** To ensure consistency and relevance of risks and their impact, we adopted the OWASP risk methodology (Tymchuk, Iepik and Sivyakov, 2017). This methodology helps organisations

estimate risk from business and technical perspectives, and it is also highly adaptable and applicable to most organisations of any sizes. In identifying relevant risks, risk sources from OWASP are considered because it maintains a regularly-updated list of most pressing cybersecurity concerns.

- **Common Attack Pattern Enumeration and Classification (CAPEC):** CAPEC provides a publicly available catalogue of common attack patterns that helps users understand how adversaries exploit weaknesses in applications and other cyber-enabled capabilities (Barnum, 2008). Attack Patterns are descriptions of adversaries' common attributes and approaches to exploit known weaknesses in cyber-enabled capabilities. Attack patterns define the challenges that an adversary may face and how they go about solving them. Each attack pattern captures knowledge about how specific parts of an attack are designed and executed and gives guidance on ways to mitigate the attack's effectiveness. Attack patterns help those developing applications or administrate cyber-enabled capabilities to understand better the specific elements of an attack and how to stop them from succeeding.
- **Common Attack Pattern Enumeration and Classification (CAPEC):** CAPEC is a structured approach for understanding how an adversary operates. It provides a comprehensive list of known attacks employed by an adversary to exploit known cyber environment weaknesses. Such a model enables the identification, classification; rating, comparison and prioritisation of security risks associated with systems and applications, and this relevant model have been adopted for threat analysis for adequate cybersecurity.

#### 4.2.4. Controls

Risk controls are generic fundamental, technical or procedural methods that are used to manage security risks. Thus, we select control measures from the predefined list provided by CIS CSC and ENISA. CIS CSC (Mbanaso, Abrahams and Apene, 2019) and ENISA are renowned industry guidelines for identifying risk control measures.

- **The Centre for Internet Security Critical Security Controls (CIS\_CSC) and ENISA:** CSC\_CIS and ENISA are used for identifying risk control measures. This is because CIS CSC provides 20 controls categorised into three prioritised and defence-in-depth best practices that are implementable to mitigate the most common attacks against systems and networks. It also provides adequate controls that organisations should take to block or mitigate known attacks into their defensive cybersecurity portfolio. Some of these controls are relevant to cybersecurity risks, while others are less relevant. Further, ENISA provides 27 baseline security controls that focus on control measures that protect computing systems against operational risks. As a result, a parallel

matching is performed for identifying semantic equivalence between controls in CSC CIS and ENISA.

#### **4.3. Integrated Cybersecurity Risk Management (i-CSR) Process**

From this research perspective, a process is considered a systematic set of activities executed towards accomplishing cybersecurity risk management. A process establishes a solid relationship between multiple steps for the effective delivery of an expected outcome. An activity deals with linked tasks that are interdependent that receive and convert one or more input into an output artefact (Knight and Burn, 2005). The process provides a means of contextualising an organisation, determining critical assets, profiling threats and vulnerabilities, profiling risks, and determining existing controls' effectiveness. The process manifests efficiency and adequacy for analysing the cybersecurity aspects of critical infrastructure and can determine the effectiveness of existing controls.

The process also provides an overview of vital phases that an organisation considers when considering the cybersecurity risk management framework. For simplification purposes, the process is decomposed into activities and steps that provide a lower level of detail, as outlined in Table 4.1. The division of the process is imperative in creating a comprehensive set of related activities that allow organisations to identify and achieve deliverables for i-CSR. Activity one and two focuses on the organisation's scope for gaining a comprehensive understanding of supported assets, functions, goals and essential security requirements. Activity three gathers vulnerability and threat information from multiple sources through various means to address vulnerabilities protect assets and respond to threats. Activity four determines the risk level and provides a risk register with the previous activities' data. Activity five implements control measures and evaluate the effectiveness of the existing control. The effectiveness of one activity determines the essential elements of information needed for the next activity. Therefore, activity five evaluates the effectiveness of the existing controls. Each activity specifies the steps that need to be followed, and each step identifies the needful inputs, participating actors and final output.

Primarily, the output of each activity serves as the input to the next activity that follows it. The process's effectiveness is mainly achieved when conducted with the support of security experts delegated by an organisation to oversee the i-CSR project. Hence, an organisation must delegate suitable actors to participate and supervise in the implementation of the process.

**Table 4.1: i-CSRМ Framework Process**

<b>Activity</b>	<b>Steps</b>	<b>Input</b>	<b>Technique</b>	<b>Performed by</b>	<b>Output</b>
Activity 1: Organisational Context	Identify actors and their roles	They are grouping the actors into internal and external. Internal actors represent the respective roles and responsibilities of personnel/departments within an organisation. External actors include stakeholders that are involved in the delivery of other services outside the organisation	Examining job profile, roles, duties and responsibilities of actors	Top management	A defined list of actor and their roles
Activity 2: Asset Identification and Criticality	Asset Profiling	An overview and list of the organisation's assets, their core functionalities and subcomponents.	Review of asset inventory, security policy, interviewing security analyst and physical observation of assets	Security Analyst and IT Manager	Description of assets, functions, and subcomponents owners, criticality and asset goals
	Identify the Asset security goals	Existing asset profile	Combination of asset control principles and organisation's security policies	Security Analyst	Enumeration of security goals and principles that each asset must achieve for sustained operations of the organisation
	Determine Asset criticality	Asset profile and goals.	Employing asset criticality ranking using fuzzy logic to determine criticality level	Security analyst	Consistent and unambiguous classification of assets according to criticality level to the organisation's processes and functions.
Activity 3: Threat Modelling	Determine Vulnerability profile	Organisational assets and list of vulnerabilities provided by CWE	Employing CWE methodology for vulnerability ranking	Security Analyst	A comprehensive vulnerability profile ranking vulnerabilities in assets according to the CWE methodology
	Determine Threat profile	Organisational assets, list of threats provided by CAPEC	Employing the CAPEC model for threat analysis	Security Analyst	A comprehensive threat profile detailing potential threats to assets according to the ATT&CK model

Activity 4: Risk Assessment	Predict Risk Types	A collection of security risks from OWASP that are associated with the threats are identified	Application of OWASP risk methodology that provides a list of risk types	Security Analyst	A detailed risk register highlighting risks types
	Risk level prediction	A collection of vulnerabilities and list of critical asset, potential threats identified and existing control measures are provided from CAPEC	Application of machine learning technique that estimates risks type and risk level	Security Analyst	A detailed risk register highlighting risks type and risk level and recommended controls
Activity 5: Risk Controls	Identify Existing Controls	A list of organisations controls detailing control functionalities	Review of control inventory and report of existing control measures	Security Analyst	A detailed control register highlighting existing controls
	Determine the effectiveness of existing Controls	The result of findings based on examining and analysing existing controls and implementing new controls from CIS CSC	Manual and automated documentation of findings	Security Analyst	A detailed control register highlighting existing controls and a list of new controls

### **4.3.1. Activity 1: Organisational context**

Every organisation exclusively operates within a defined scope and available resources. Organisational context tends to better understand the organisation's existing state by providing the essential elements of information needed to give an i-CSRM framework proper direction to be achieved successfully. The organisational context involves identifying its significant stakeholders, actors, critical assets, security goals and how they impact risk management and viability. A stakeholder is any entity with a conceivable interest or stake in an activity (Goodpaster, 1991). A stakeholder can be an individual, group of individuals, or an institution affected by or influences an activity's impact. Stakeholders are actors such as top management and administrators. Who are directly or indirectly involved in influencing the success of the organisation and its processes. To successfully execute the process and achieve this activity, it is essential to obtain a comprehensive picture of actors and their roles in meeting requirements. This becomes important in identifying and avoiding a potential conflict of interests and other issues such as the actors responsible for the security and maintenance of organisations assets.

#### **4.3.1.1. Step 1: Identification of Actors and their roles**

An actor represents an entity such as an organisation or human user with a strategic goal within its organisational setting, carries out specific activities and makes informed decisions. Actors interact with the organisation's systems or relationships by providing technical and nontechnical support or services to the organisation. The nature of communications between actors needs to be clearly balanced, reconciled, interpreted and managed accordingly. The organisation's activities require an active set of actors to carry out various tasks to guide and lead the organisation in achieving its goals and ensuring its successful operations. In this case, actors can be identified as internal and external actors. The internal actor is the organisation itself that supply infrastructure, network facilities and other services needed to run its operations and has skilled personnel who play different roles such as information technology security analyst, risk manager and senior engineer. External actors mainly include users who use the organisation's services and third-party vendors who provide other services such as internet services.

### **4.3.2. Activity 2: Asset Identification and Criticality**

This activity aims to identify and prioritise assets in terms of their boundary, components and assigning weights to the assets based on the organisation's importance. Assets are specific units such as hardware, a database, application, or program that support the delivery and usage of an organisation's services.

Furthermore, to support organisations in assessing each asset's criticality, a decision support system using fuzzy set theory is created. A fuzzy set theory provides a way of absorbing the uncertainty

inherent to phenomena whose information is unclear and uses a strict mathematical framework to ensure precision and accuracy and the flexibility to deal with both quantitative and qualitative variables (Zimmermann, 2011). It can be used for approximate reasoning, easy to implement and adopt individual perception without incurring complexity within the risk management process. This activity includes three steps; identify assets and their goals, determining asset criticality, and identifying the business process. The resulting critical asset list is then used to assess vulnerability assessment and threat identification in Activity 3.

#### **4.3.2.1. Step 1: Asset Profile**

This step's basis is to profile assets in terms of their components, boundaries and assigning weight to the assets based on assets vital to the organisation. Assets are specific units such as a database, application, or program that support the delivery and usage of an organisation's services. To create asset profiles, a Security Analyst is involved in identifying assets by considering the core functions of the assets, alongside other subcomponents essential to achieving and maintaining crucial functions. Important asset information can be gathered by reviewing background materials, including independent audit/analytical reports, interviewing the critical infrastructure users, and physical observation of organisational assets. Besides, asset specification and management documentation provide essential details about the organisational asset.

#### **4.3.2.2. Step 2: Identify Asset Security Goals**

Security asset goals are specific attributes that describe assets expected conformance to secure behaviour: they are also referred to as security principles. Identifying assets security goals is vital for an organisation to determine what critical views of security must be ensured by each asset during processing, storage, or transmission by authorised systems, applications, or individuals. Also, asset security goals are used in determining the impact that may result from accessing assets in an unauthorised manner for use, interruption, change, disclosure. Therefore, the Security Analyst considers a set of security goals that each asset aims to achieve. The consequential impact that may ensure the compromise of the security goals and the level of protection needed can be easily determined. There are different asset categories we consider for asset criticality. They include; software, data, hardware, information communications and network and people. We further defined a set of asset security goals every asset must aim to achieve, such as;

- **Asset Availability (A):** Availability refers to ensuring that an asset is made available and accessible to authorised users when and where they need it.
- **Asset Integrity (I):** Asset integrity refers to an asset's ability to perform its required functions effectively and efficiently without disrupting or losing its services.

- **Asset Confidentiality (C):** Asset confidentiality refers to assets staying secured and trusted and preventing unauthorised disclosure of sensitive data.
- **Accountability (ACC):** This asset goal requires that attack or incident actions that occur on an asset are tractable to the responsible system or actor.
- **Conformance (CON):** This asset goal ensures that the assets such as services meet the specified standard.

#### 4.3.2.3. Step 3: Determine Asset Criticality

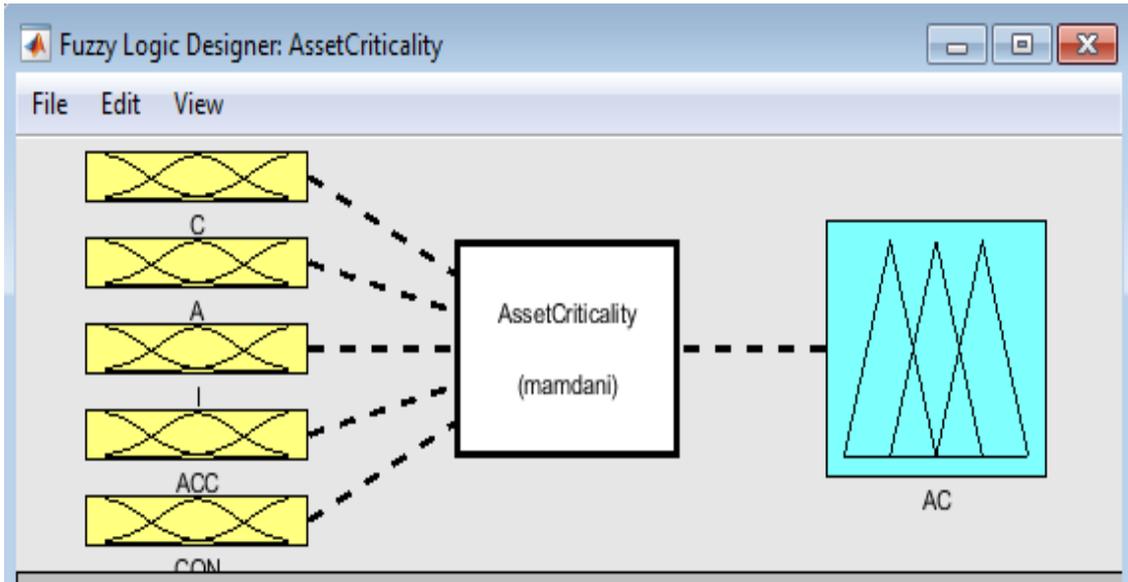
This step aims to identify and prioritise an organisation's critical asset by assessing those assets' primary security goals. In other words, the criticality of each asset is based on its relative importance. Asset criticality is imperative for prioritising and developing actions that will reduce risks to the asset, improve asset reliability, and define strategies for implementing the appropriate controls. To ensure validity, consistency, and support stakeholders in assessing each asset's criticality, a decision support system using fuzzy set theory is created. Fuzzy set theory plays a vital role in the decision process enhancement. It helps to deal with or represent the meaning of vague concepts, usually in situation characterisation such as linguistic expressions like "very critical". Fuzzy logic, introduced by (Zadeh, 1988), is one of the best ways to deal with all types of uncertainty, including lack of knowledge or vagueness (Markowski and Mannan, 2009). This system provides a methodology for computing directly with the word. Fuzzy set theory is a generalisation of classical set theory that provides a way to absorb the uncertainty inherent to phenomena whose information is vague and supply a strict mathematical framework to ensure precision and accuracy, as well as the flexibility to deal with both quantitative and qualitative variables (Zimmermann, 2011).

##### 4.3.2.3.1. Development of a Fuzzy Asset Criticality System (FACS)

Criticality is the primary indicator used to determine the importance of the assets to the organisation. After the different assets have been identified, we determine the criticality based on their relative importance using Fuzzy Asset Criticality System (FACS).

- **Fuzzification:** FACS determines asset criticality by using (C, I, A, CON and ACC) as the five fuzzy inputs for assessing the criticality of individual assets and assigning a level of criticality. Each input is assigned five fuzzy labels Very Low (VL), Low (L), Medium (M), High (H) and Very High (VH), for assessing the level of the fuzzy output Asset criticality (AC) value which is assigned five fuzzy labels Very Low Critical (VLC), Low Critical (LC), Medium Critical (MC), High Critical (HC) and Very High Critical (VHC) of individual assets. The details of fuzzy sets applied in the first step of the fuzzy inference system are presented in Table 4.2.

Figure 4.1 shows the structure of the FACS.



**Figure 4.21** Structure of the Fuzzy Asset Criticality System (FACS)

Table 4.2 shows the numerical ranges in which fuzzy sets are selected based on them. The membership functions for AC also are depicted on a scale of 1 to 5.

**Table 4.2:** Fuzzy Ratings

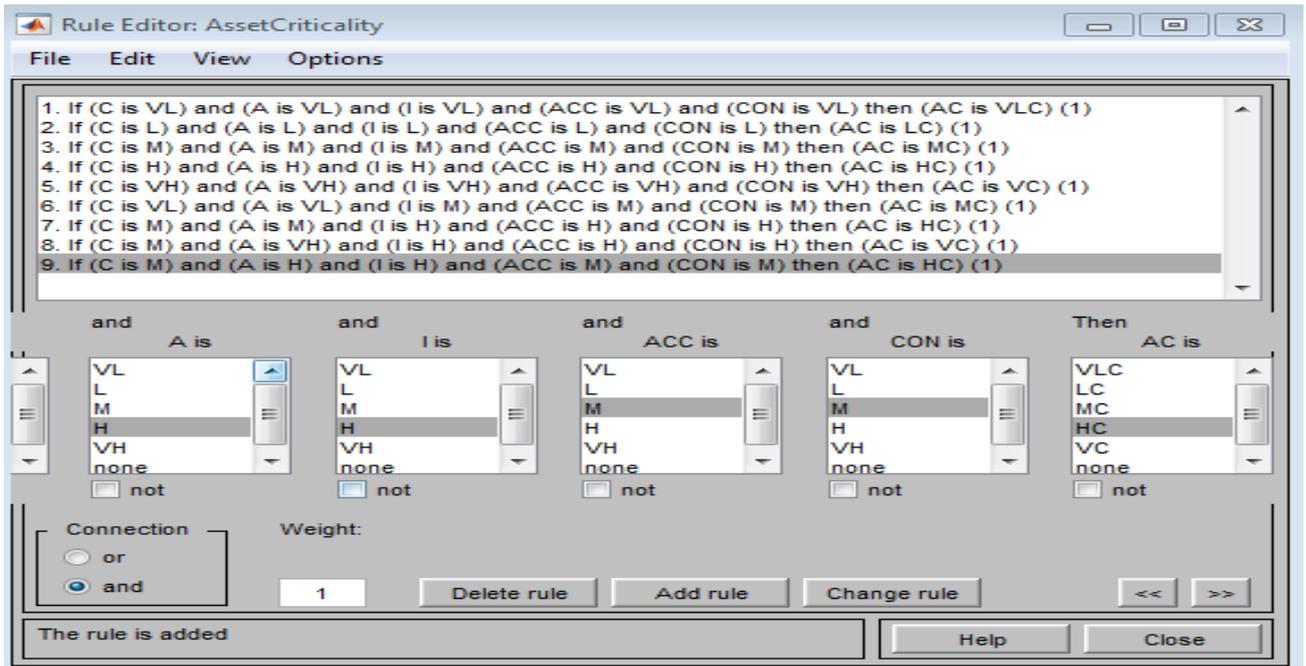
Features	Asset Factors	Description	Linguistic Terms	Crisp Rating	Interpretation
Input	Confidentiality (C)	How much data could be disclosed, and how sensitive is it?	Very High (VH)	5	All data disclosed
			High (H)	4	Extensive critical data disclosed
			Medium (M)	3	Extensive non-sensitive data disclosed
			Low (L)	2	Minimal critical data disclosed
			Very Low (VL)	1	Minimal non-sensitive data disclosed
	Availability (A)	How many services could be lost, and how vital is it?	Very High (VH)	5	All services completely lost
			High (H)	4	Extensive primary services interrupted
			Medium (M)	3	Extensive secondary services interrupted
			Low (L)	2	Minimal primary services interrupted
			Very Low (VL)	1	Minimal secondary services interrupted
Integrity	How much data	Very High (VH)	5	All data corrupt	

	(I)	could be corrupted, and how damaged is it?	High (H)	4	Extensive seriously corrupt data
			Medium (M)	3	Extensive slightly corrupt data
			Low (L)	2	Minimal seriously corrupt data
			Very Low (VL)	1	Minimal slightly corrupt data
	Accountability (ACC)	Are the threat actors traceable to an individual?	Very High (VH)	5	Completely anonymous
			High (H)	4	Fully traceable
			Medium (M)	3	Highly traceable
			Low (L)	2	Possibly Traceable
			Very Low (VL)	1	Minimal Traceable
	Conformance (CON)	How much deviation from specified behaviour constitutes conformance?	Very High (VH)	5	Full variation
			High (H)	4	High profile variation
			Medium (M)	3	Clear variation
			Low (L)	2	Low variation
			Very Low (VL)	1	Very low variation
	<b>Output</b>	Asset Criticality (AC)	How critical is the asset to the organisation?	Very Critical (VC)	5
Highly Critical (HC)				4	High importance to the organisation and requires a high level of protection.
Medium Critical (MC)				3	The asset is moderately important to the organisation and requires moderate protection
Low Critical (LC)				2	The asset is of minimal importance and does not require many levels of protection.
Very Low Critical (VLC)				1	The asset non-critical and requires a very low level of protection

- **Rules:** There are many fuzzy inference methods; however, this research uses the Min-Max fuzzy inference method proposed by Mamdani (Cordón, 2011). This research employs Mamdani's method due to several advantages (Cord, 2001):
  - It is suitable for engineering systems because its inputs and outputs are real-valued variables
  - It provides a natural framework to incorporate fuzzy IF-THEN rules from human experts

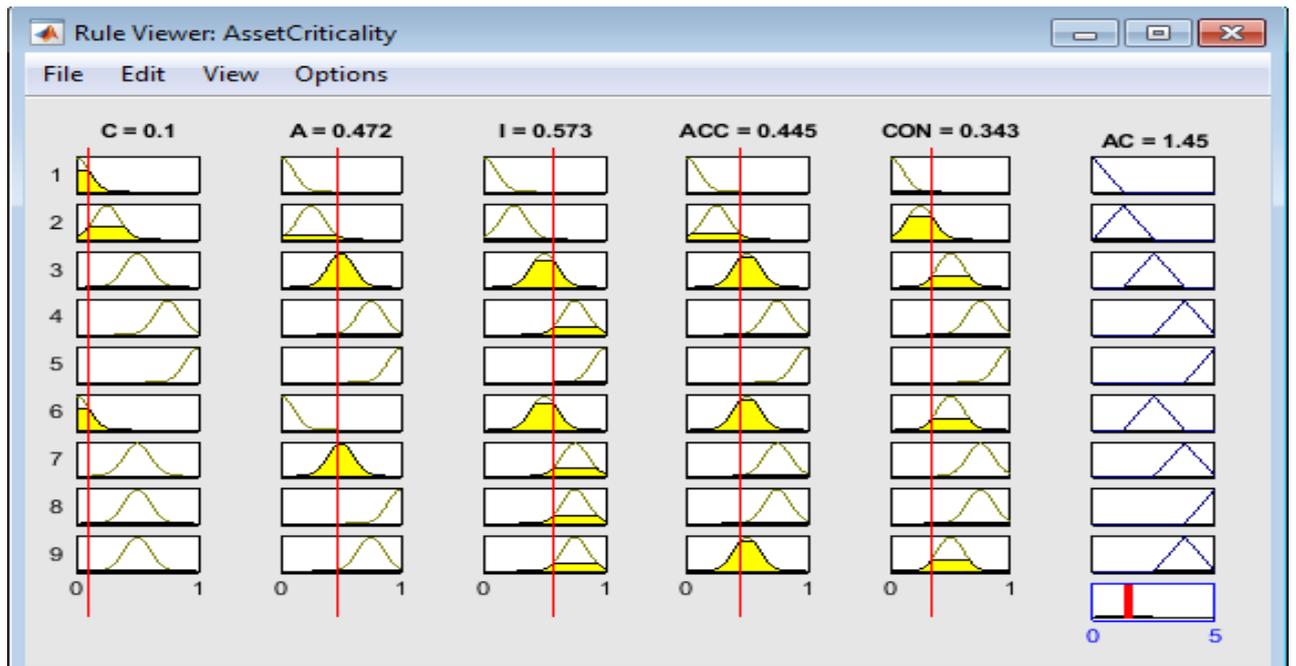
- It allows for a high degree of freedom in the choices of fuzzifier, fuzzy inference engine, and defuzzifier so that the most suitable fuzzy logic system for a particular problem is obtained. It provides a natural framework to include expert knowledge in the form of linguistic rules.

We used 125 IF-THEN rules to provide a database by mapping five input parameters (C, A, I, CON and ACC) and AC value. The rules are designed to follow the logic of the Asset criticality evaluator. A number of the IF-THEN rules of the developed system are shown in Figure 4.2.



**Figure 4.2:** Rules Set for FACS to generate a new conclusion

- **Inference Engine:** An inference engine attempts to create solutions from the database. In this paper, the inference engine maps fuzzy input sets (C, A, I, ACC and CON) into fuzzy output set (AC). Figure 4.3 shows several IF-THEN rules to provide a more understanding of the proposed FACS model.



**Figure 4.3:** Sample of Rules

- **Defuzzification:** Different methods for converting the fuzzy values into crisp values such as Centre of Gravity (COG), Maximum Defuzzification Technique and Weighted Average Defuzzification Technique. For this research, we used the most commonly used defuzzification method known as COG. The COG technique can be expressed as follows:

$$X^* = \frac{\int \mu_i(x)xdx}{\int \mu_i(x)dx} \text{ (Equation 4.1) (Chakraverty, Sahoo and Mahato, 2019)}$$

Where  $x^*$  is defuzzified output,  $\mu_i(x)$  is aggregated membership function, and  $x$  is the output variable.

#### 4.3.3. Activity 3: Threat Modelling

Threat modelling activity focuses on identifying and measuring vulnerabilities and threats related to the assets. The Security Analyst performs this activity. Based on the previous activity's assets, all possible threats that could impact the assets negatively are profiled in a register. However, effective identification and control of threats require an understanding of threat sources, threat actor behaviour, capability and intent (Workman, Bommer and Straub, 2008). Only through an understanding of the current threat landscape can organisations know about the nature of threats they face and the control measures to implement. In other words, a holistic understanding of threats enables a more effective prioritisation of control actions and decision making. This is possible when known attack patterns employed by the threat actor to exploit vulnerabilities are known to allow an organisation to understand and create a threat profile expansively. Because of these considerations, this activity has

created two steps for threat modelling: (i) the determination of Vulnerability profile; and (ii) the determination of threat profile.

#### 4.3.3.1. Step 1: Determine the Vulnerability profile

Determining the vulnerability profile is vital because it allows for identifying and assessing vulnerabilities associated with critical assets. This step aims to identify potential asset vulnerabilities that a threat actor may leverage to exploit an asset. It is an essential and delicate task that has an impact on the successful operation of critical infrastructures. A sound approach that enables gathering valuable insights based on the analysis of situational and contextual vulnerabilities that can be tailored to the organisation-specific threat landscape is used.

Hence, the Common Weakness Enumerator (CWE) methodology (Martin, 2007) is used to determine the vulnerability factors as a publicly known vulnerability source. Therefore, to estimate the likelihood of risk, it is necessary to estimate a particular vulnerability discovered and exploited. We adopt CWE, which allows for weaknesses to be characterised, allowing stakeholders to make informed decisions when mitigating risks caused by those weaknesses. Each related weakness is mapped to CAPEC and identified by a CWE identifier and the name of the vulnerability type. The CWE gives a general description, behaviour, likelihood of exploit, consequences of exploit, potential mitigation and related vulnerabilities. To apply the CWE methodology, a rating table is presented in Table 4.4 with corresponding values assigned to the different factors that can help organisations determine the likelihood of risk. Each option has a likelihood rating from 0 to 9, and the overall likelihood falls within high, medium and low, which is sufficient for the overall risk level. The Security Analyst could explore other publicly available sources of vulnerability information, including internal experience, penetration test, vulnerabilities catalogues available from industry bodies, national government, and legal bodies. The questions can also be extended to meet the organisation's need.

**Table 4.4: Vulnerability Factor Rating**

Vulnerability Factors	Vulnerability ID	Description	Likelihood rating	
			Weight	Value
Ease of discovery	EoD	How easy is it for vulnerability to be discovered?	1	Practically impossible
			3	Difficult
			7	Easy
			9	Automated tools available
Ease of exploit	EoE	How easy is it for vulnerability to be exploited?	1	Theoretical
			3	Difficult
			5	Easy
			9	Automated tools available
Awareness	Awa	How well known is this vulnerability to the threat actors?	1	Unknown
			4	Hidden
			6	Obvious
			9	Public knowledge
Intrusion	I_D	How likely is an exploit to	1	Active detection in

detection		be detected?		application
			3	Logged and reviewed
			8	Logged without review
			9	Not logged

#### 4.3.3.2. Step 2: Determine Threat profile

Determining the threat profile is essential because it allows for the identification and understanding of threat characteristics. To determine threats, it requires a structured representation of threat information that is expressive and all-encompassing due to the dynamic and complex nature of a CPS. A Security Analyst must use a sound approach that enables gathering valuable insights based on the analysis of situational and contextual threats that can be tailored to the organisation-specific threat landscape. A method that could be used is MITRE's models for the threat intelligence sharing called CAPEC and WASC. Therefore, this step effectively identifies the threat types, target assets, threat actor factors, TTP, and compromise indicators likely to affect a critical infrastructure's ability to deliver its services.

CAPEC is an acronym formed from the first letter of Common Attack Pattern Enumeration and Classification used to define the potential threat, provide context for architectural risk analysis, and understand trends and attacks to monitor. Also, WASC stands for Web Application Security Consortium. Hence, the Security Analyst could explore publicly available sources of threat information. For example, we recommend that threat information approved by CAPEC (Barnum, 2008) and WASC (Consortium, 2009) be followed because there are several threats identified in these two sources. Besides using the CAPEC and WASC models, actors use the following procedure to create a comprehensive threat profile:

- **Threat type:** To create a comprehensive threat profile, organisations need to identify the potential threats of assets that a threat actor may leverage to attack. The Security Analyst needs to back up his claim with a solid foundation of Information sources.
- **Threat Actor factors:** Effective identification and control of threats require an understanding of threat sources, threat actor behaviour, skill, resources required, capability and intent (Workman, Bommer and Straub, 2008). Therefore, we adopt the OWASP methodology that considers various threat actor factors such as; skill level, size, motivation, location, resources, and opportunity to understand the attack and its trend. Using these threat actor factors, the Security Analyst can determine the likelihood of an attack and the severity of the threat. This will provide the ability to create an impact rating for threats. Table 4.5 shows the threat actor factors, and each factor has a set of options with a likelihood rating from 0-9.

**Table 4.5:** Threat Actor Factors Rating

Threat Actor factors	Description	Likelihood rating	
		Weight	Value

Skill level	How technically skilled is the threat actor?	1	No technical skills
		3	Some technical skills
		5	Advanced computer user
		6	Network and programming skills
		9	Security penetration skills
Location	Through what channel did the threat actor communicate to reach the vulnerability?	1	Internet
		8	Intranet
		8	Private Network
		7	Adjacent Network
		5	Local Network
Motive	How motivated is the threat actor to find and exploit the vulnerability?	2	Physical
		1	Low or no reward
		4	Possible reward
Resources	What resources are required for the threat actor to find and exploit the vulnerability?	9	High reward
		0	Expensive resources required
		4	Special resources required
		7	Some resources required
Opportunity	What opportunities are required for the threat actor to find and exploit the vulnerability?	9	No resources required
		0	Full access required
		4	Special access required
		7	Some access required
Size	How large is the group of the threat actor?	9	No access required
		2	Developers
		2	Systems administrators
		4	Intranet users
		5	Partners
		6	Authenticated users
		9	Anonymous internet users

- **Determine Tactics, Techniques and Procedures (TTP) and Indicator of Compromise (IOC):** TTP and IOC involve the pattern of activities used by a threat actor to plan and manage a cyber attack, thereby compromising critical assets. The different TTP types include; *initial access, execution, credential access, persistence, privileged escalation, defence evasion, collection, lateral movement, exfiltration and command and control*. The different IOC includes; *network indicators, email indicators and host indicators*. Therefore, we adopt the ATT&CK (adversarial tactic, techniques and common knowledge) framework developed by MITRE to document standard TTP used to target, compromise and operate in an enterprise network. To calculate the risk level and know the appropriate controls to protect the organisation's assets, information about TTP must be known. Table 4.6 shows the possible TTP and IOC that are frequently employed when exploiting the vulnerability.

**Table 4.6:** TTP and IOC (Tactic, 2017)

Tactics type	Techniques	Procedure	IOC
Initial access	Spearphishing link	It employs links to download malware in an email by electronically delivering social engineering targeted at a specific individual or organisation.	Email, Network
	Drive-by compromise	A threat actor gains access to a system by visiting a website over the ordinary browsing course. The	Network

		website is compromised where the threat actor has injected some malicious code.	
	Replication through removable media	The threat actor uses a tool to infect connected USB devices and transmit them to air-gapped computers when the infected USB device is inserted.	Host
	Spearphishing attachment	A threat actor attaches and sends a Spearphishing email with malicious Microsoft office attachment and requires user execution in order to execute.	Email
Execution	Command-line interface	The threat actor uses a command-line interface to interact with systems and execute other software during operation.	Host
	Dynamic data exchange (DDE)	Threat actor sends a Spearphishing containing malicious word document with DDE execution.	Host, Network
	Execution through module load	The threat actor uses this functionality to create a backdoor through which it can remotely load and call dynamic link library (DLL) functions.	Host
	Exploitation for client execution	Threat actor exploits a vulnerability in office applications, web browsers or typical third party applications to execute the implant into the victim's machines.	Network
Persistence	Account manipulation	Threat actor adds a created account to the local administrator's group to maintain elevated access.	Host, Network
	Accessibility features	The threat actor uses a combination of keys known as the sticky keys to bypass a user's windows login screen on remote systems during the intrusion.	Host, Network
	Component firmware	Threat actor overwrites the firmware on a hard drive by compromising computer components.	Host, Network
Privilege escalation	External remote services	Threat actors leverage legitimate credentials to log into external remote services	Host, Network
Defense evasion	Disabling security tools	Threat actor disables the windows firewalls and routing before binding to a port.	Host, Network
Credential access	Brute force	Threat actor brute forces password hashes to be able to leverage plain text credentials.	Host, Network
Discovery	Network sniffing	The threat actor uses a tool to capture hashes and credentials sent to the system after the name services have been poisoned.	Host, Network
	Network service scanning	Threat actor used BlackEnergy malware to conduct port scans on a host.	Host
	System information discovery	The threat actor uses tools such as systeminfo that obtains information about the local system.	Host
Lateral movement	Remote services	The threat actor uses putty secure copy client (PSCP) to transfer data or access compromised systems.	Host
	Third-party software	Threat actor distributes malware by using a victim's endpoint management platform.	Host
Collection	Data from information repositories	Threat actor collects information from Microsoft SharePoint services using a SharePoint enumeration and data dumping tool within target networks	Host, Network
	Email collection	The threat actor uses utilities to steal email from archived outlook files and exchange servers that have not yet been archived.	Email, Host, Network
	Man in the browser	The threat actor uses a Trojan spyware program to perform browser pivot and inject into a user's browser and trick the user into providing their login credentials on a fake or modified web page.	Network
Exfiltration	Data encrypted	The threat actor uses malware such as duqu to push and execute modules that copy data to a staging area, compress it, and XOR encrypts it.	Host
Command and control	Commonly used port	The threat actor uses duqu, which uses a custom command and control protocol that communicates over	Network

		commonly used ports and is frequently encapsulated by application layer protocols.	
	Remote file copy	The threat actor used Shamoon malware to download an executable to run on the victim.	Network

#### 4.3.4 Activity 4: Risk Assessment

The output of threat modelling provides a list of vulnerabilities, related vulnerabilities, potential security threats, and assets' impact. The threat register serves as a help to the Security Analyst to orchestrate a risk register's creation and focus on the most potent threats. This activity allows for establishing the risk assessment context by following the threat register and formally approves the risk management activities within the organisation. The activity provides various additional estimations required for the risk evaluation by enabling the determination of risks that are likely to occur, the severity of the risks, and the steps to control or manage the risks. This requires the top management and risk manager's active involvement to emphasise the importance of risk assessment to the organisation. This activity's output is a risk register, and the overall risk impact level falls within high, medium and low. This ensures that minor risks are not prioritised, while more severe risks are overlooked. The first step of this activity identifies risk types. Secondly, it identifies existing controls and lastly calculates risk impact value.

##### 4.3.4.1. Step 1: Predict Risk Types

This step proposes using machine learning techniques for predicting risk type so that appropriate mitigation processes can be implemented. In this context, risk type prediction relies on a pioneering mathematical model such as machine learning for analysing, compiling, combining and correlating all incident-related information and data acquired from previous activities. The machine learning (ML) techniques automatically find valuable underlying patterns within i-CSRMs concepts used as features, and then the patterns predict risk types. The i-CSRMs features are considered input for the ML classifiers and ML classifiers to predict the risk type. Therefore, we used well-known classifiers such as K-Nearest neighbours (KNN), Naïve Bayes (NB), the Naïve Bayes Multinomial (NB-Multi), Neural Network (NN) with Ralu activation function at activation layers and sigmoid function at the output layer, Decision Tree (DT), Random Forest (RF), and Logistic Regression (LR) for risk type prediction. There are five phases to achieve this step, and they are explained in chapter 5, section 5.2.

We present data extraction to generate a feature set, which is then further used on the ML classifiers for training purposes. Finally, the test data is used to check the accuracy of the prediction. Figure 4.4 shows how these features are used to train the classifiers and the step by step process of the risk prediction, i.e. the experiment in general. Data collection and extraction were considered from the dataset; feature extraction was carried out on those data and used to train the ML classifiers (NN, RF, LR, NB-Multi DT, KNN and NB). The data were further partitioned into 80% training and 20%

testing. We used the random partition (divide 80% data into the training set and 20% into the testing set), and reported the average results obtained over the ten folds. Predictions are carried out on the testing dataset, and accuracy measures the prediction.

Also, risks types from multiple industry bodies can be considered because they maintain a regularly updated list of most pressing security risks. For example, the Common Attack Pattern Enumeration and Classification (CAPEC) provide a comprehensive list of risks that can be used for understanding and enhancing defense. All these sources can be used.

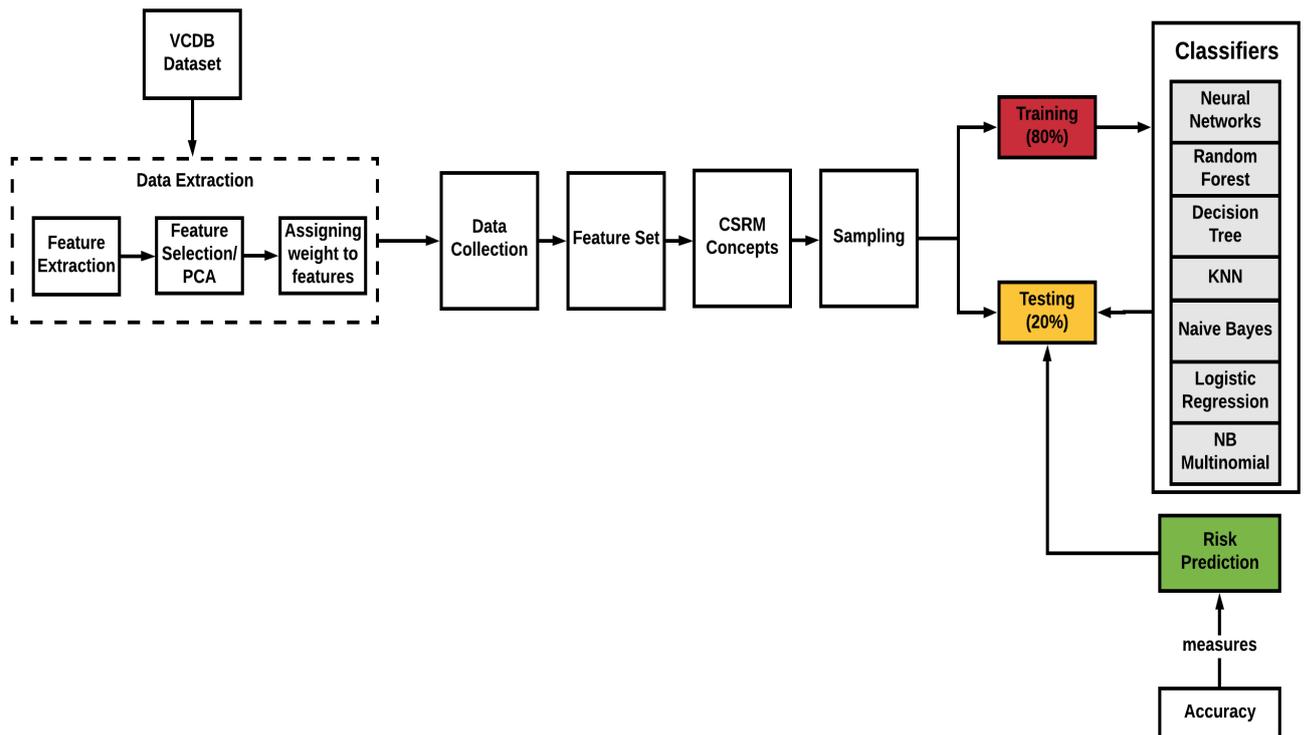


Figure 4.4: Classification process about the primary analysis and methods that have been used to build the experiment

#### 4.3.4.2. Step 2: Determine Risk Level

After information about the potential risk types, threat, vulnerabilities and assets have been identified and gathered, and the next step is to determine the risk level of all the possible risk types predicted. The risk level is usually not known and not estimated correctly. In essence, organisations need to rate security risks that have been identified. Therefore, for the risk level to be estimated, we used the technical impact factors. The technical impacts factors are inclined toward an asset's security goals that include; confidentiality, integrity, availability, accountability, and conformance. Also, information about the threat actor and vulnerability factors needs to be gathered. The aim is to

provide a rough estimate of the risk level's magnitude if a risk occurs. The equations follow the OWASP methodology for assessing risk (Wichers, 2013).

**Phase 1:** To estimate the overall (L) Likelihood of the risk, threat actor factors and vulnerability factors are put into consideration, as shown in Equation 4.2. Each option has a likelihood rating from 0 to 9, as shown in Table 4.4 and 4.5. The overall likelihood falls within high, medium and low, sufficient for the overall risk score. Table 4.8 shows the overall likelihood level.

$$L = \frac{TAF + VF}{2} \quad (\text{Equation 4.2})$$

**Where:**

*L* = Likelihood

*TAF* = Threat Actor Factors,

*VF* = Vulnerability Factors

$$TAF = SL + L + M + Res + Opp + S / n \quad (\text{Equation 4.3})$$

**Where:**

*SL* = Skill Level

*L* = Location

*M* = Motivation

*Res* = Resource

*Opp* = Opportunity

*S* = Size

*n* = total number of TAF factors (6)

$$VF = EoE + EoD + Aw + ID / n \quad (\text{Equation 4.4})$$

**Where:**

*EoE* = Ease of Exploit

*EoD* = Ease of Discovery

*Aw* = Awareness

*ID* = Intrusion Detection

*n* = total number of VF factors (4)

**Table 4.8:** Overall Likelihood Rating

Likelihood	Rating
Low	0.00 – 2.99
Medium	3.00 – 5.99
High	6.00 – 9.00

**Phase 2:** To Estimate the overall ( $Impact_F$ ) impact of a successful attack, we consider the total loss of the asset's goals, as shown in Equation 4.5. Each factor has a set of options with an impact rating from 0 to 9, as shown in Table 4.9.

$$Impact_F = AF/n \quad (\text{Equation 4.5})$$

**Where:**

$Impact_F$  = Impact Factor

$AF$  = Asset Factors ( $L_C + L_A + L_I + L_{ACC} + L_{CON}$ )

$L_C$  = loss of Confidentiality

$L_A$  = loss of Availability

$L_I$  = loss of Integrity

$L_{ACC}$  = loss of Accountability

$L_{CON}$  = loss of Conformance

$n$  = Total number of the Technical factors (5)

**Table 4.9:** Impact Factors

Impact Factors	0 to < 3 (Low)	3 to < 6 (Medium)	6 to 9 (High)
Loss of Confidentiality	Minor disclosure of critical assets	Critical assets are significantly affected	Highly critical assets are extensively affected
Loss of Integrity	Minor compromise of critical assets	Critical assets significantly compromised	All highly critical asset extensively compromised
Loss of Availability	Minor interruption of critical assets	Critical assets significantly interrupted	All critical assets extensively lost
Loss of Accountability	Threats are fully traceable	Threats are possibly traceable	Threats are completely untreatable
Loss of Conformance	A minor breach of compliance requirements	A significant breach of compliance requirements	All compliance requirements significant breached.

Table 4.10 shows the overall  $Impact_F$  level.

**Table 4.10:** Overall  $Impact_F$  Rating

Likelihood	Rating
Low	0.00 – 2.99
Medium	3.00 – 5.99
High	6.00 – 9.00

**Phase 3: Determine Risk Severity:** To determine the risk level, we estimate the likelihood and impact are combined to calculate the overall severity of risk using Equation 4.6.

$$R_{Level} = L * Impact_F \quad (\text{Equation 4.6})$$

**Where;**

$R_{Level}$  = the risk level

$I$  = the impact of the asset goals

$L$  = the likelihood of the attack occurring within a given time-frame

Overall risk severity is rated as high, medium, or low, as shown in Table 4.11 below.

**Table 4.11: Overall Risk level**

Overall Risk level	
00 – 20	Low
21 - 45	Medium
46 – 65	High
66 – 81	Critical

**4.3.5 Activity 5: Risk Controls**

There is a need to identify and implement controls that can be used to address the risks. Risk controls are generic fundamental technical or procedural mechanisms that are used to manage security risks. This activity displays the current risk status for each risk event, together with their calculated risk values. The Security Analyst needs to identify the potential control measures that can be used to mitigate the risks based on the risk level. Therefore, risk assessment plays a critical role in this activity. The Security Analyst considers various industry standards that provide recommendations on basic security controls. For example, the Critical Security Controls (Mbanaso, Abrahams and Apene, 2019) publishes a set of 20 controls and best practice guidelines that organisations should adopt to control known computer security risks. Thus, we recommend that the Security Analyst selects risk control measures from the predefined list provided by a renowned industry guideline named CSC CIS to define control measures. CSC CIS provides 20 controls categorised into three prioritised and defence-in-depth set of best practices that are implementable and usable to mitigate attacks against systems and networks.

In selecting the controls, the security Analyst uses the matching process to compare the security control measures from the different standards and identify and filter controls that have similarities, i.e. controls that complement each other in terms of scope. The elements used for the comparison include the name of the control measure, type, and keywords. In such cases where control measures are the same, the Security Analyst should adopt CSC CIS controls. However, if there is no similarity, control measures from both CSC CIS and other standards should be adopted. This approach ensures that contents are compared more thoroughly and risk control actions consistently and easily identified.

Therefore, this activity's primary objective is to specify essential risks controls and evaluate the effectiveness of the existing control measures that protect assets to ensure sufficient coverage in the management of critical infrastructure.

#### 4.3.5.1. Step 1: Identification of Existing Control Types

There is a need to identify a list of existing controls that are in place to address risks before risk level is identified. Therefore, this step identifies the existing controls and categorises them into corrective, detective and preventive actions to mitigate the risk. The risk impact level will determine those not adequate controls so that new controls can be implemented.

#### 4.3.5.2. Step 2: Evaluating the Effectiveness of Existing Controls

This step involves assessing the effectiveness of existing controls, determining each control's level, and avoiding unnecessary duplication of controls if existing controls are not adequate and new controls need to be implemented. Therefore, a check should be made to ensure that the controls are working correctly. If a control does not work as expected, this may cause vulnerabilities leading to risks. Consideration should be given to the situation where a selected control fails in operation, and therefore complementary controls are required to address the identified risk effectively. In assessing the effectiveness of existing controls and determining each control's level, an assessment of each control objective is carried out by an assessor team. The controls are evaluated in terms of relevance, strength, coverage, integration, and traceability according to ISO 27005:2011 standard (*GOST, 2009*). For each criterion, a rating score from 1 to 5 is given to measure which control addresses the specific control objective. Table 4.13 shows the five different criteria rating.

**Table 4.13: Criteria Rating**

<b>Rating</b>		<b>Description</b>
5	Adequate control	The control achieves the objectives intended to mitigate the risks.
4	Adequate control with some areas of improvement	The control achieves the objectives intended to mitigate the risks with evidence of some areas, though not critical, subject to improvement to meet sound controls' requisites.
3	Generally adequate control, with some critical areas	The control mostly mitigates the risks intended to mitigate the risks. However, the characteristics of some of the controls are not entirely consistent with basic sound controls
2	Inadequate control, subject to significant improvement	The control partially achieves the control objectives intended to mitigate the risks
1	Insufficient control	The control is not sufficient to achieve the control objectives intended to mitigate the risks.

Table 4.14 shows the overall effectiveness of the controls.

**Table 4.14:** Overall effectiveness

Description	Overall Effectiveness
Insignificant	0-5
Minor	6-10
Moderate	11-15
Major	16-20
Critical	21-25

To find the overall evaluation of each control, Equation 4.7 is given:

$$OE = R + S + C + I + T \quad \text{(Equation 4.7)}$$

**Where:**

*OCE = Overall Control Effectiveness*

*R = Relevance*

*S = Strength*

*C = Coverage*

*I = Integration*

*T = Traceability*

#### **4.3.5.3. Step 3: Implement Control Measures to Determine New Risk Status**

Table 5.16 presents the control measures implemented in three levels represented in three different colours. The green ones are fully implemented to reduce the risk value evenly. The yellow ones are only partially implemented and reduce the risk value by half of a green one. The red ones do not reduce the risk at all. Therefore, this step involves performing appropriate analysis to measure which control addresses which risk. Criteria, each criterion help the assessment; a rating score from 0 to 9 is given to measure which control addresses the specific control objective. The security Analyst can select the control measure rating. It further displays the current risk status for each risk type. It presents the risk events and their calculated risk values, and the control measures that can be used to mitigate the risk.

#### **4.3.5.4. Risk Register**

A risk register is an important document that provides a tentative record of potential risks in line with vulnerability and threat profile, assets and security goals. The risk register displays the results of the risk calculation. Each risk event is evaluated and presented in a table and the elements used in the calculation, and the calculated risk value. The calculated risk value represents how dangerous the risk

event might be for the organisation. The presented risk events are then sorted from the most dangerous to the least dangerous, ensuring that minor risks are not prioritised while more severe risks are overlooked.

## CHAPTER FIVE

### Evaluation of the Integrated Cybersecurity Risk Management Tool (i-CSRMT)

#### 5.1. Introduction

The previous Chapter presented the i-CSRMT process, which comprises various essential activities and steps. This Chapter presents an Integrated Cybersecurity Risk Management Tool (i-CSRMT) to support organisations' risk management activities. The tool's objective is to minimise the time and efforts required to perform the proposed risk management activities in Chapter five and provide accurate information about risks based on the cyber-attack that occurred and affects the organisation's assets so that the organisation can make an informed decision. It provides a comprehensive workflow to guide the user through the individual activities, starting with identifying the actors and their roles within the organisation, identifying critical assets, revealing the hazardous threats, risk calculation and finishing with control evaluation. The tool can be simultaneously accessed and used by multiple users and different organisations and simultaneously manages multiple different projects. The tool also provides a separate web interface for the different actors within the organisation (application administrators), giving them access to the user and project management.

In this Chapter, the architectural and critical design of i-CSRMT is presented in detail, which is categorically designed to support critical infrastructures in risk management performance. In plain terms, i-CSRMT is designed to serve as a platform by which an organisation can assess its critical assets, identify vulnerabilities and threats, calculate risks levels, and evaluate its existing controls' effectiveness to implement informed decisions. The primary objective of i-CSRMT is to facilitate the collection of threats and analysis of risks, including the establishment of subjective judgment and determination of the required course of actions that needs to be taken, thereby promoting cybersecurity in critical infrastructures.

#### 5.2. Overview of i-CSRMT

The i-CSRMT tool is an implementation of the i-CSRMT process. This tool designed to support i-CSRMT framework activities that an organisation uses to perform security risk analysis, in particular, critical infrastructures. It provides a comprehensive workflow to guide the user through the individual activities, starting with identifying the actors and their roles within the organisation, identifying critical assets, revealing the particularly dangerous threats, risk calculation and finishing with control evaluation. This helps to minimise the efforts required to perform the risk management activities and provide accurate information about the risk level based on the CTI context to implement the proper controls. It is also designed to enable organisations to use threat intelligence report to predict a certain risk level. Another critical aspect of i-CSRMT is that it is formed based on the principles of renowned

industry-standard. Also, the tool can be simultaneously accessed and used by multiple users and different organisations and allows managing multiple different projects simultaneously. The tool also provides a separate web interface for the different actors within the organisation (application administrators), giving them access to the user and project management. Therefore the tool aims for an effective risk management practice within a real-life context.

### **5.3. General Description of i-CSRMT Tool**

The i-CSRMT is a web-based front end written in PHP (Lerdorf, Tatroe and MacIntyre, 2006), HTML5 (Hickson and Hyatt, 2011), JavaScript, and MySQL database (Glass et al., 2004). A standard browser will view the client-side, and it will be able to operate on any web server that supports JavaScript, PHP, and MySQL. Administrative, user, actor, activities, and vendor modules make up the system. Java Server Pages (JSP) (Hall and Brown, 2001) is used for the managerial and user interfaces, and MySQL is used for retrieving, adding, removing, and updating data throughout the database. This design allows several users to log in and communicate with the tool at the same time.

Furthermore, i-CSRMT was built with two interface types in mind: administrative and user. The administrator is a type of user, and he or she has the right to install and adjust system settings and user rights. The second kind of user consists of staff who can only execute activities that the supervisor has delegated to them. The tool is made up of many separate modules that may be used individually depending on the user's access privileges. The application's user interface is made up of a collection of related web pages that can be reached directly from the navigation menu on the left side of the application. Each web page is associated with certain aspects of risk management activity and provides essential functionalities to manage evidence collection, analysis, and report generation. Notably, the web pages interact with one another through a MySQL-based shared database.

### **5.4. Design process**

In designing i-CSRMT, important considerations are made regarding the most vital aspects of the risk management activity and forming the tool's features around these considerations. Several architectural designs were considered, including a distributed system that utilises client-server web service technology and distributed systems using PHP and JavaScript. For each architectural design, the pros and cons were considered, including feasibility and capability to cope with the tool's features. For example, the architectural pattern in web services technologies is lightweight. Distributed systems create more cohesion and increase the degree of interdependence between modules. PHP and JavaScript are the server-side scripting language that is independent, multi-platform, and would allow the tool to be more coupled, which implies that the client will be more dependent upon the server-side. Therefore, after thorough consideration and proof of concepts, it is decided for the tool to be implemented as a client-server web system designed using PHP and JavaScript.

## **5.5. Architecture of i-CSRMT**

In this section, the architecture of the tool is explained. i-CSRMT is a simple three-tier, web-based system that uses a client-server architecture. A three-tier architecture is an architecture pattern for developing web applications that work around three critical layers, comprising a presentation layer, application layer and data layer (Machado, Filho and Ribeiro, 2009). The application architecture is in many ways inspired by the Domain-Driven Design (Evans, 2004) and was developed using the Java programming language. From a logical point of view, three-tier architecture is used to improve the tool's modularity and mainly allow for easy extension of features. Using client-server architecture, users can use any web browser to connect to the many services supported by the tool, such as initiating audit assessments. On the server-side, the web server receives requests from the client, handles the request and generates an appropriate response to the client. The three-tier architecture role of three-tier architecture is explained as:

### **5.5.1. Presentation Layer**

This layer manages the communication with the Web browser, renders the application Web pages, and controls the user access. The layer consists of a single module that represents the user interface. It is implemented using the Java Play Framework (Leroux and Kaper, 2014) and follows the Model-View-Controller (Enache, 2015) architectural pattern. The Views represent the contents of the application Web pages and are built using HTML, PHP, CSS and JavaScript. Some Views contain only parts of the user interface; either embedded into the Web pages or loaded dynamically using AJAX. The server's communication is managed using Controllers, which handle the HTTP requests and return responses in rendered Views.

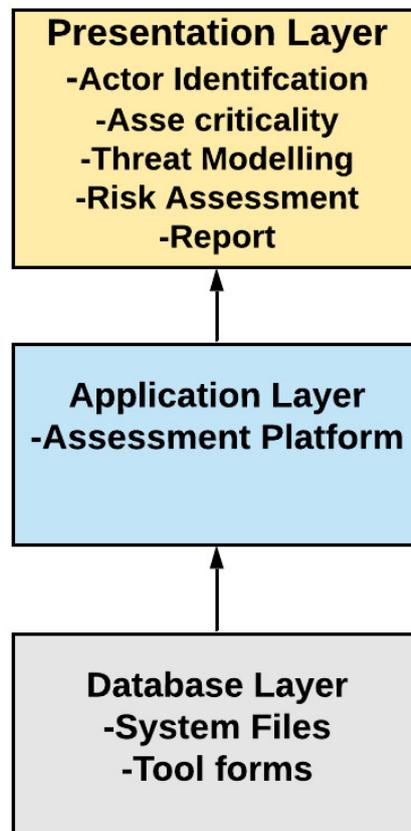
### **5.5.2. Application Layer**

The application layer is built using PHP and it plays the role of linking together all the three layers by technically processing the various inputs and selections received at the presentation layer and interacting with the vast database in the third layer. Also, the layer houses the web server, scripting language and the scripting language engine of the tool. The Web server enables the processing of HTTP requests for initiating the activity process. The application layer provides the technical deal with dynamic content and streamlines the database's faster access to extract results.

### **5.5.3. Database Layer**

The database provides a centralised place where data captured in the tool are stored, manipulated, and accessed. The layer comprises database management systems (DBMS) and the database, which is built using MySQL. The database layer's rationale is to centralise all data storage, store and retrieve the application data. In other words, it contains the methods for accessing the underlying database data. Fundamentally, the database layer is responsible for storing numerous types of data the tool will

take as an input, generate as output and other external services that the tool may use. The database is accessible to the system administrators and employees. The high-level architecture for the tool is shown in Figure. 5.1.



**Figure 5.1:** Architecture of i-CSRMT

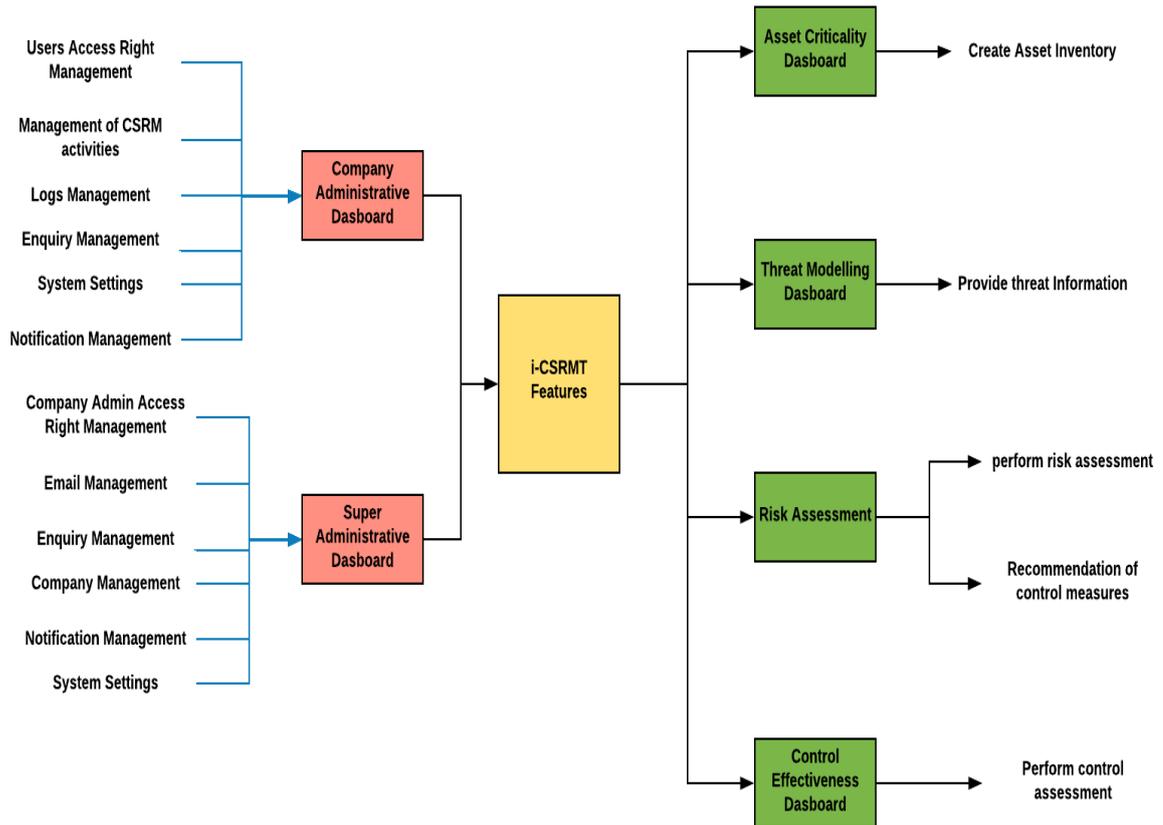
### 5.6. i-CSRMT Features

This section provides a detailed overview of i-CSRMT features. The application Web pages are organised according to the previously defined workflow activities in Chapter five. They were created focusing on user cooperation, which allows the users to split their work and delegate responsibilities. The application administrators can define dynamic user roles and assign them to the users to restrict their access to specific application parts. The primary purpose is to provide a general understanding of how the tool is decomposed and how the individual components work together to provide the desired functionalities. In general, the tool focuses on minimising the efforts required to perform the risk management activities and provide accurate information about the risks. The tool's main features include a main dashboard consisting of essential functions that can be performed. Each functionality contains essential components of a risk management process. The main features include;

- Actor identification

- Asset criticality
- Threat modelling,
- Risk assessment,
- Control effectiveness
- Report dashboard

Figure 5.2 shows the main features of the i-CSRMT.



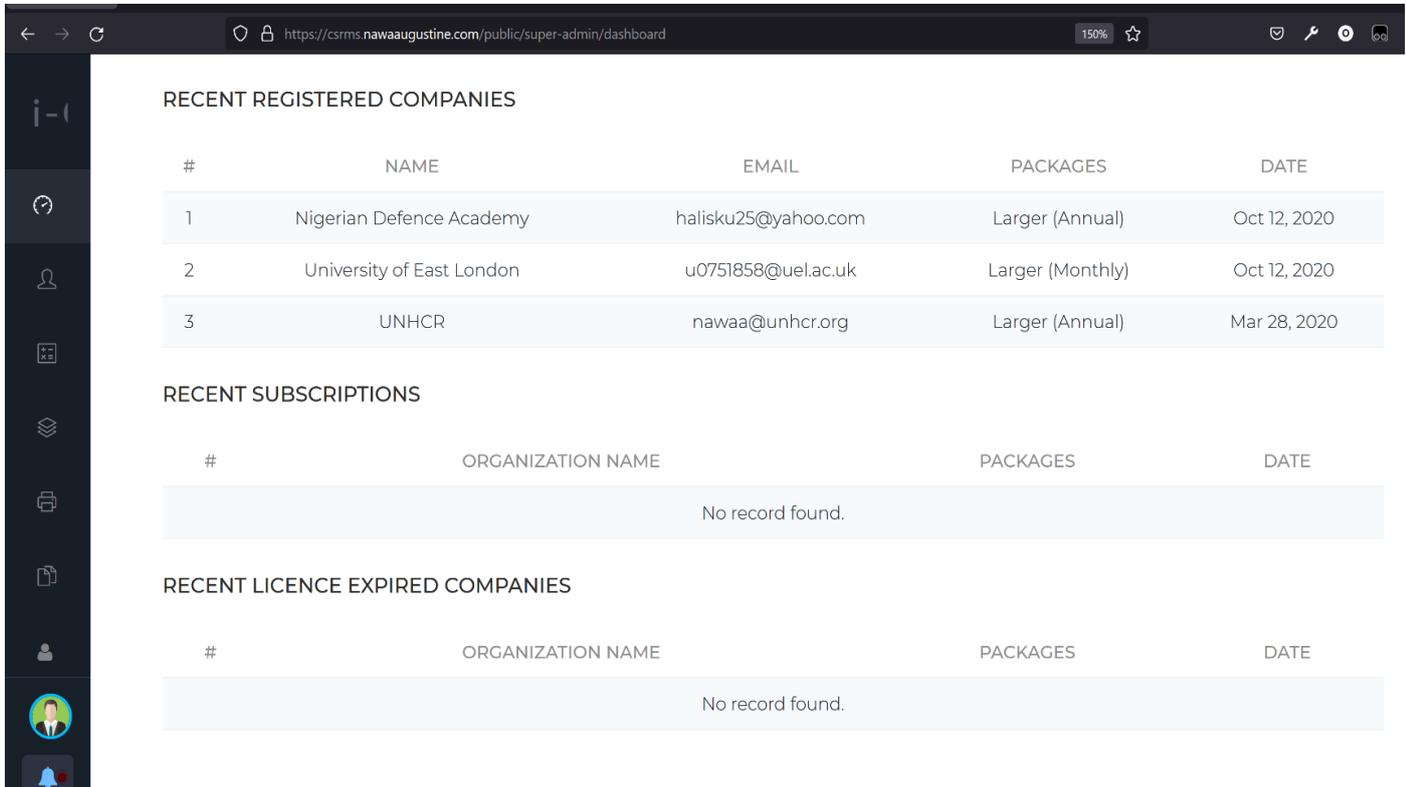
**Figure 5.2:** Features and components of i-CSRMT

### 5.7. Dashboard Views

A preliminary view of the powerful dashboards in i-CSRMT is presented in this section. The interface uses a straightforward, plain layout with very little or no graphics. Information is displayed very clearly to users through HTML pages, with visualisation mechanisms that present information using visual aids such as charts. As mentioned earlier, the central dashboards in i-CSRMT are six and screenshots from these dashboards are provided below:

### 5.7.1. Super Administrator Dashboard

A preliminary view of the super administrator dashboard in i-CSRMT is presented in this section. The dashboard displays the total companies created, number of active companies, number of inactive companies, total packages, and companies with expired licenses. To the left are the menu options navigable to linked pages and with various tasks



**Figure 5.3:** Super Administrator Dashboard

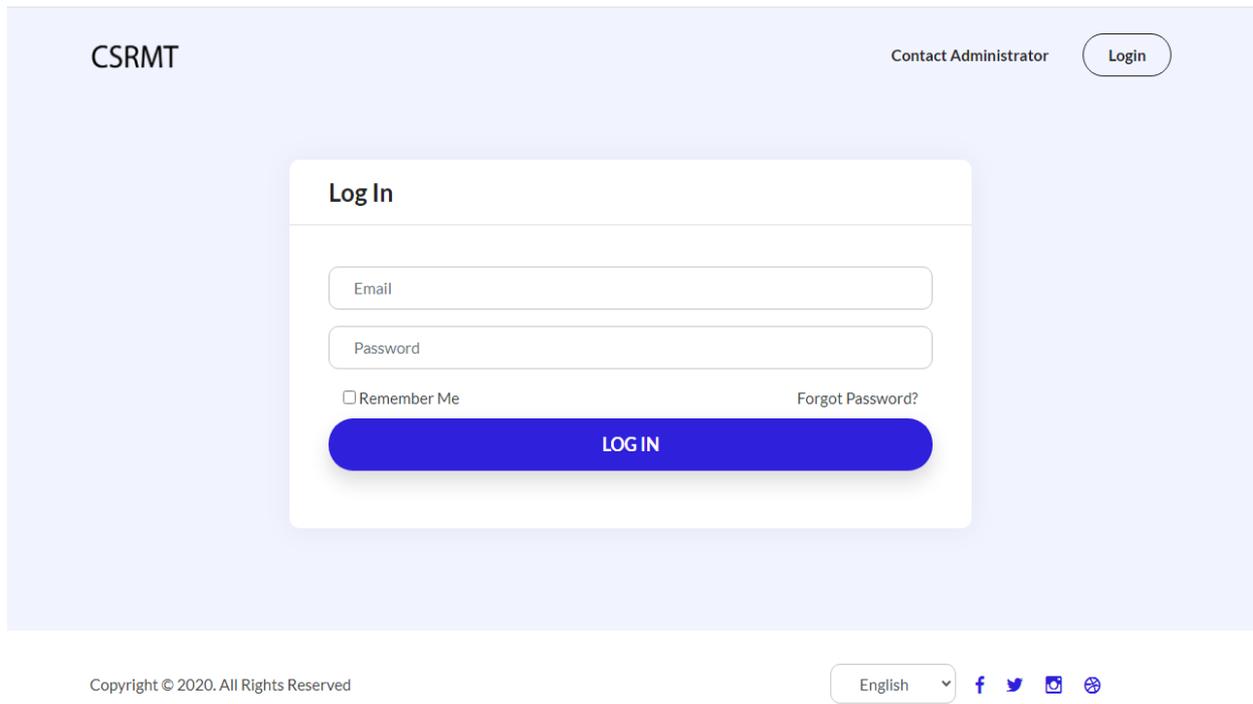
#### 5.7.1.1. Super Admin Login

This page enables the i-CSRMT super administrator to log in with a valid and authorised email address and password to carry out the task of creating and registering new companies, manage invoices (if the company is paying), manage subscriptions, perform global settings on the application and other essential tasks on the dashboard. This page uses a sha256 Salt Hash Security mechanism to run a session check and transmit a valid or invalid result.

*URL: <http://csrmt.org/public/login>*

*Email: [ocjpnawa@gmail.com](mailto:ocjpnawa@gmail.com)*

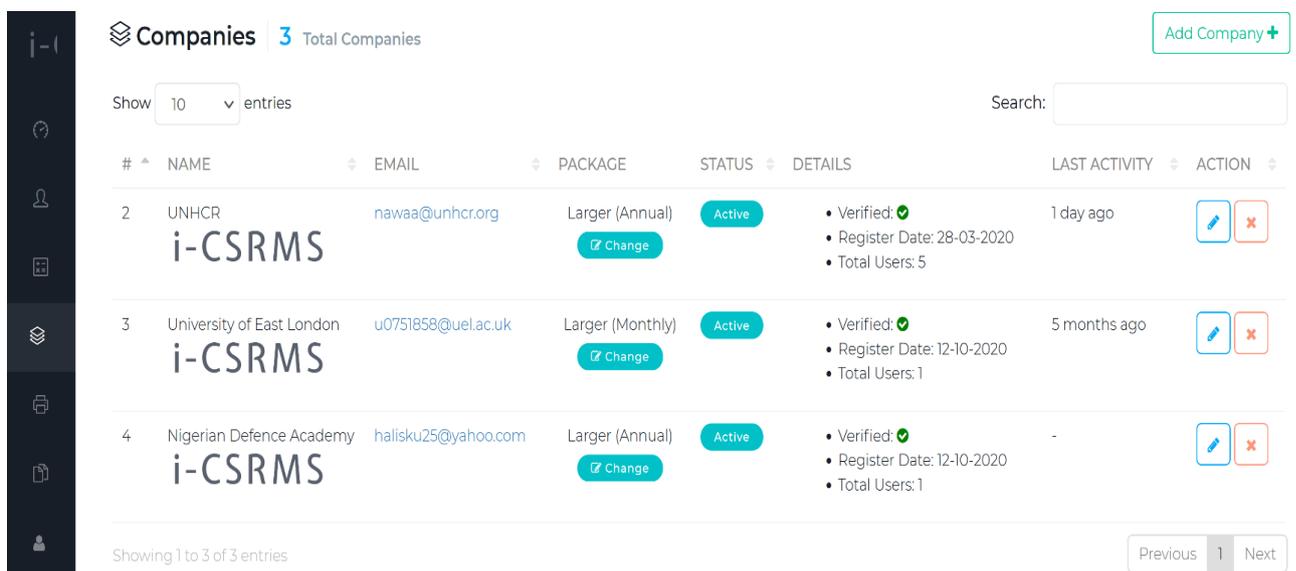
*Password: Nawa@123*



**Figure 5.4: Super Admin Login**

### 5.7.1.2. Super Admin Manages Company

This page allows the super admin to edit, delete or add new companies. The super admin adds the companies' details such as; organisation name, email, website, logo, address, and phone to add a new company. It also allows the super admin to create account details such as the new organisation's username and password. The new organisation will receive an email notification with a username and password and use the details to login to the tool to carry out their risk assessment tasks. The organisation can change its password if they wish.



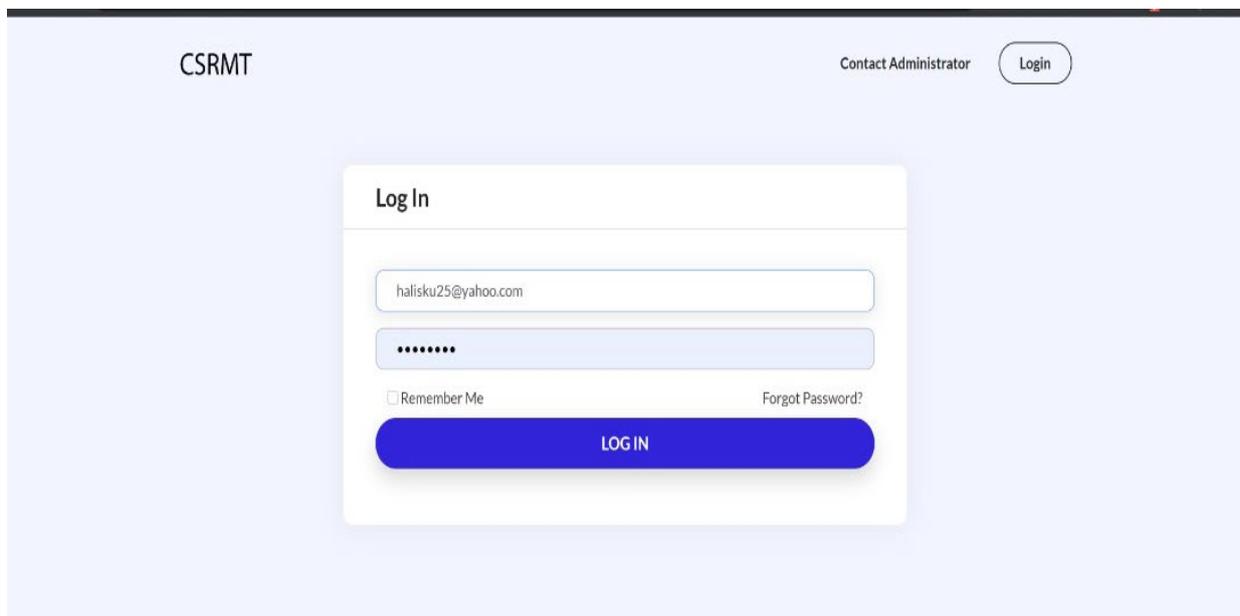
**Figure 5.5:** Super Admin Manages Company

### 5.7.2. Company Administrator Dashboard

This feature aims to provide administrative and user management functions in terms of authentication and providing actors access to the i-CSRMT platform. The authentication module is designed using PHP, JavaScript with MySQL database, which serves as an integral part of security procedures. This dashboard's primary user is the i-CSRMT administrator, who creates user accounts for all authorised actors and vendors. The admin dashboard also enables the company admin to manage logs and user activities to review employee activities and vendors. The company administrator can add, remove or edit the list of actors, projects and vendors that can use the tool, in addition to password recovery capabilities. Among other functions, the administrative dashboard allows the company admin to maintain the overall system security, carry out risk analysis, functionalities and definition of user access rights; create actor and company admin account; control of project platform; verification of Vendor's details; notification services on completed projects, in-progress projects, cancelled projects, overdue projects, total projects and not started projects.

#### 5.7.2.1. Admin Login

This page enables the i-CSRMT administrator and all other users to log in with valid and authorised email address and password to carry out the task of administering essential tasks on the dashboard. The super administrator creates new company login details for the company admin.



The screenshot displays the Admin Authentication form within the CSRMT system. The page header includes the text "CSRMT" on the left, "Contact Administrator" in the center, and a "Login" button on the right. The main form is titled "Log In" and contains the following elements: an email input field with the text "halisku25@yahoo.com", a password input field with masked characters "\*\*\*\*\*", a "Remember Me" checkbox, a "Forgot Password?" link, and a prominent blue "LOG IN" button.

**Figure 5.6:** Admin Authentication form

### 5.7.2.2. Company Administrator Homepage

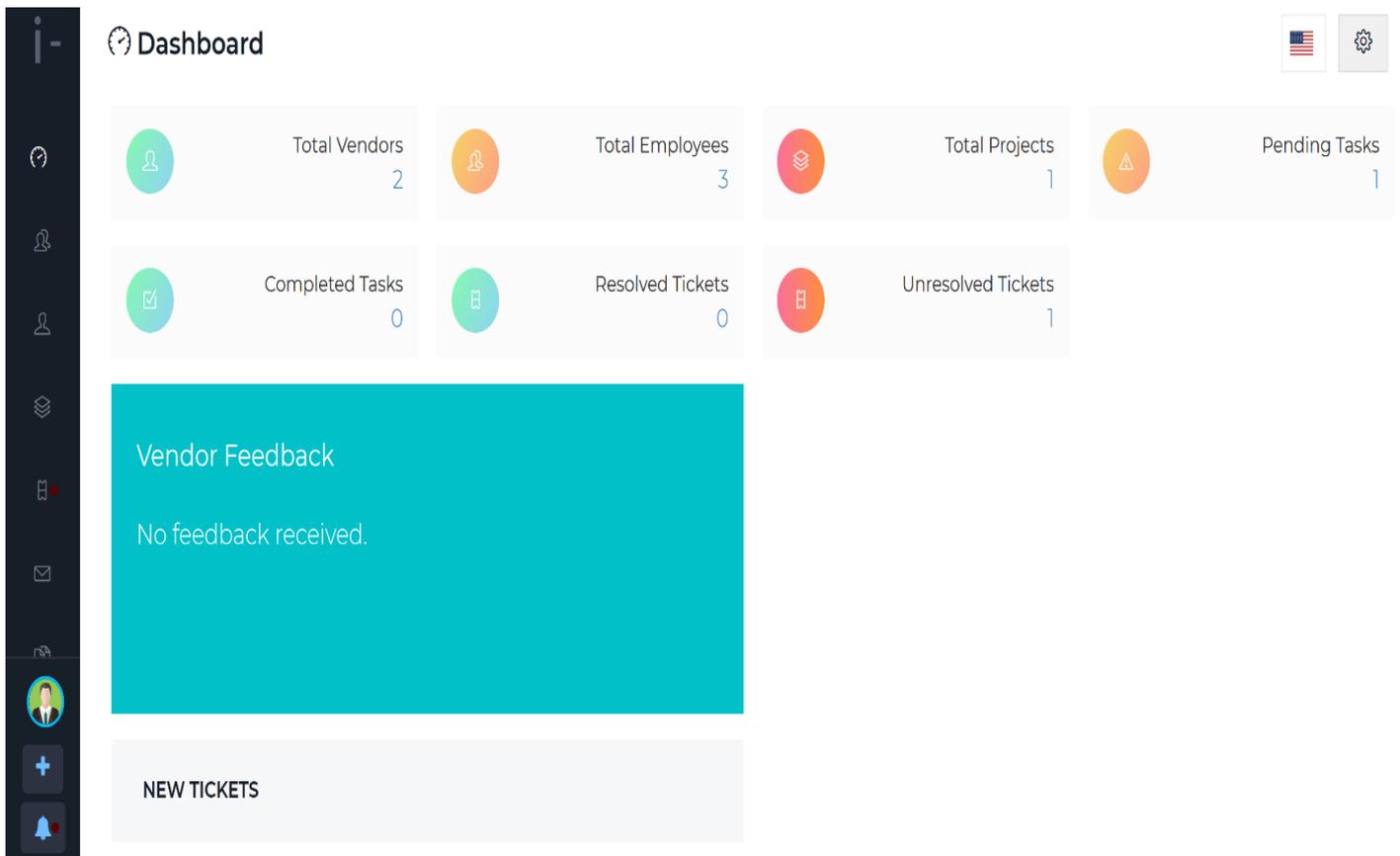
The Company Admin login with initial username and password sent to their email by the super admin. The company admin is advised to request a new password the first time they login. This is the official landing page of the company admin if successfully logged in. The company Admin dashboard provides the primary features of the assessment. It comprises the data display sheet with total vendors, total employees, total project, pending project and completed tasks.

Furthermore, this page enables the company Admin to add new company vendors. Furthermore, manage the company vendor's account. This section enables the admin to keep track of the Vendor's particular task or action. It shows the total number of vendors added and when i-CSRMT us of the Vendor if active or not—also, the log of the time and date of when the Vendor was created and actions performed.

*URL: <http://csrmt.org/public/login>*

*Email: [nawaa@unhcr.org](mailto:nawaa@unhcr.org)*

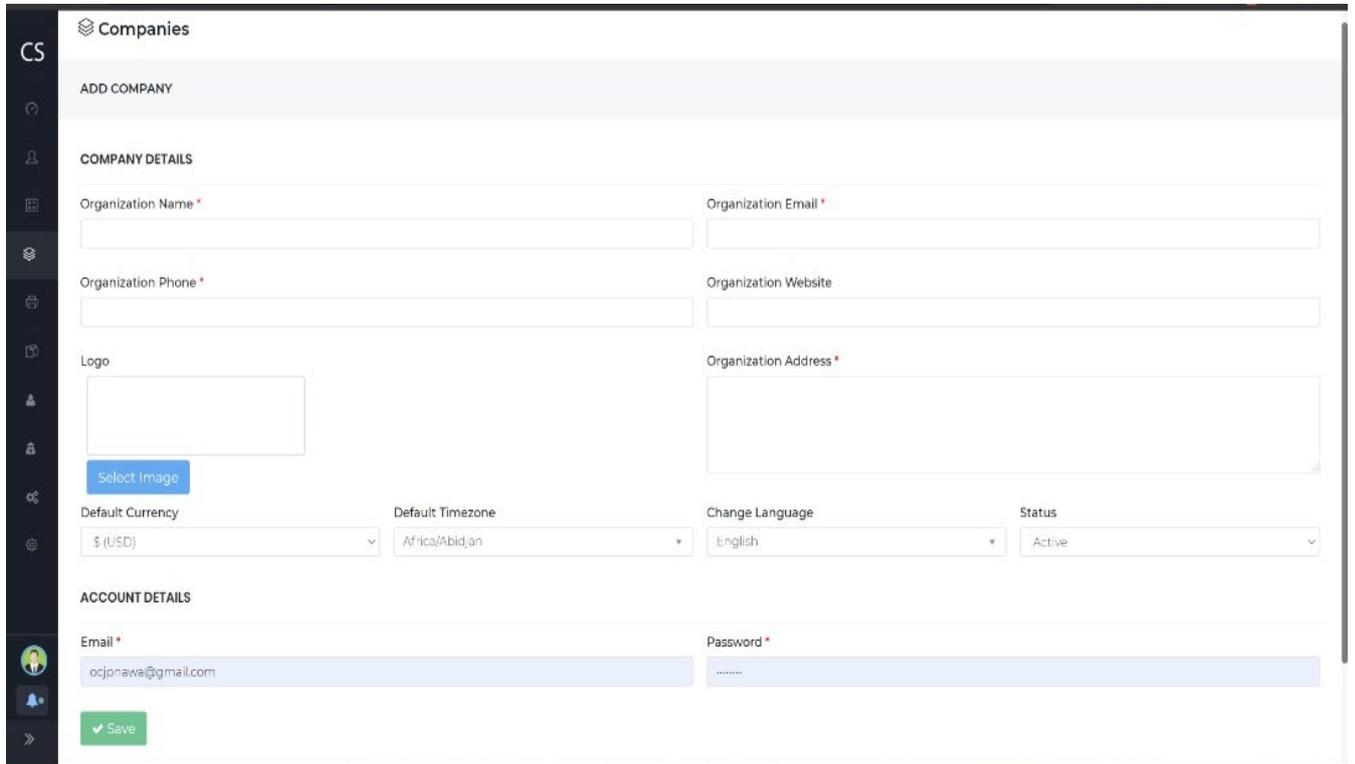
*Password: Nawa@123*



**Figure 5.7:** Company Admin Homepage

### 5.7.2.3. Add Company Details

This page enables the admin to add and save company details such as organisation name, website, email, and telephone number. To the left are the menu options navigable to linked pages and with various tasks. The admin creates a new company page by filling in the form and saving it.



The screenshot shows a web application interface for adding company details. The page is titled "Companies" and "ADD COMPANY". The form is divided into several sections:

- COMPANY DETAILS:**
  - Organization Name \* (text input)
  - Organization Email \* (text input)
  - Organization Phone \* (text input)
  - Organization Website (text input)
  - Logo (image input with "Select Image" button)
  - Organization Address \* (text input)
- Configuration:**
  - Default Currency: \$ (USD) (dropdown)
  - Default Timezone: Africa/Abidjan (dropdown)
  - Change Language: English (dropdown)
  - Status: Active (dropdown)
- ACCOUNT DETAILS:**
  - Email \* (text input, value: ocjonawa@gmail.com)
  - Password \* (password input, value: .....

A green "Save" button is located at the bottom left of the form.

Figure 5.8: Add Company details

### 5.7.3. Identification of Actors and Role Dashboard

This homepage enables the company Admin to add new employees, delete and edit existing employees. Also, the company admin selects roles for each employee within the organisation to enable the system to create a new user account based on the assigned role. Furthermore, the company Admin groups users into various departments and assign a designation. The admin can create, edit and delete departments and designations.

**Employees** Add New Employee +

3 Total Employees | 3 Not working on project

Show 10 entries | Search:

ID	NAME	EMAIL	USER ROLE	STATUS	CREATED AT	ACTION
1	Admin	nawaa@unhcr.org	Role of this user cannot be changed.	Active	28-03-2020	
2	Shola Risk Manager	shola@campustechng.com	<input type="radio"/> Admin <input type="radio"/> Employee <input type="radio"/> IT Manager <input checked="" type="radio"/> System Analysts <input type="radio"/> Security Analysts <input type="radio"/> System Administrator <input type="radio"/> Registered Users <input type="radio"/> IT Managers	Active	28-06-2021	

**Figure 5.9: Actors and Role**

### 5.7.3.1. Adding and Managing Actors Roles

This page enables the admin to add new roles within the organisation and manage existing roles by either deleting or editing the roles.

**Roles & Permissions** Manage Role

IT Manager	0 Member(s)	Permissions
System Analysts	1 Member(s)	Permissions
Security Analysts	0 Member(s)	Permissions
System Administrator	0 Member(s)	Permissions
Registered Users	0 Member(s)	Permissions
IT Managers	1 Member(s)	Permissions
Risk Manager	0 Member(s)	Permissions

**Figure 5.10: Adding and Managing Actors Roles**

### 5.7.3.2. Roles and Permissions

This page allows the admin to define the type of permission associated with that role. Furthermore, employees can now be added and assigned to the different roles created.

The screenshot displays the 'Roles & Permissions' management interface. On the left, a sidebar lists various settings, with 'Roles & Permissions' highlighted. The main area shows two roles: 'IT Manager' (0 members) and 'System Analysts' (1 member). Below the roles is a table for managing permissions for various entities.

<input type="checkbox"/> SELECT ALL	ADD	VIEW	UPDATE	DELETE
Clients	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Employees	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Projects <b>1</b>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Tasks <b>1</b>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Risk Assessment	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Controls Effectiveness	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Tickets <b>1</b>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**Figure 5.11:** Actors Roles and Permissions

### 5.7.4. Managing Project Dashboard

This section enables the Company Admin to add new projects, view archives and select a project template. All activities are grouped as a single project. The Company Admin can see completed, cancelled, in progress, not started, the overdue and total number of projects entered. Furthermore, different project members can be added to the project with different activities assigned to them.

## Projects

[View Archive](#)[Project Templates +](#)[Add New Project +](#)

2 Total Projects

2 Overdue Projects

0 Not Started Projects

0 Completed Projects

2 In Progress Projects

0 Canceled Projects

Show 10 entries

Search:

ID	PROJECT NAME	PROJECT MEMBERS	DEADLINE	VENDORS	COMPLETION	STATUS	ACTION
1	IT Infrastructure project for DISCOS		20-04-2020	Test Vendor	Progress 0%	In Progress	...
2	NIIT		22-05-2020	Test Vendor	Progress 0%	In Progress	...

Showing 1 to 2 of 2 entries

Previous 1 Next

Figure 5.12: Managing Projects

### 5.7.4.1. Asset Inventory

This page enables the administrator to create an asset inventory of all the organisation's assets by adding the different assets' name. Furthermore, this feature allows the system to automatically evaluate critical assets by selecting "Confidentiality (C), Availability (A), Integrity (I), Accountability (ACC) and Conformance (CON) as five inputs for assessing the criticality of individual assets and assigning a level of criticality. Each input is assigned five labels; Very Low (V), Low (L), Medium (M), High (H) and Very High (VH), for assessing the level of the output. The total returns a criticality value of very Low (V), Low (L), Medium (M), High (H) or Very High (VH) for each of the assets.

# Asset Inventory

Create Asset



Show 10 entries

Search:

ID	ASSETS TITLE	ASSET CONFIDENTIALITY	ASSET AVAILABILITY	ASSET INTEGRITY
25	HR system developed in PHP	All data disclosed (5)	All services completely lost (5)	All data corrupt (5)
24	HTML website	All data disclosed (5)	All services completely lost (5)	All data corrupt (5)

Figure 5.13: Managing Asset Inventory

### 5.7.4.2. Threat Modelling

After the Assets have been added to the tool, this page automatically displays the types of threats that are likely to affect the assets and compromise sensitive information. The page displays the threat name, description of the threat, resources required, skills required, indicators of compromise, TTP, related attack pattern and the possible vulnerabilities. This page automatically pulls data from the CAPEC dataset to fetch the different threat types associated with the asset's assets in the asset inventory page. The tool pings the CAPEC dataset at the interval to fetch new data if it has been updated.

### THREAT MODELLING

**Threat Name**  
Cross Site Tracing

**Description**  
Cross Site Tracing (XST) enables an adversary to steal the victim's session cookie and possibly other authentication credentials transmitted in the header of the HTTP request when the victim's browser communicates to destination system's web server. The adversary first gets a malicious script to run in the victim's browser that induces the browser to initiate an HTTP TRACE request to the web server. If the destination web server allows HTTP TRACE requests, it will proceed to return a response to the victim's web browser that contains the original HTTP request in its body. The function of HTTP TRACE, as defined by the HTTP specification, is to echo the request that the web server receives from the client back to the client. Since the HTTP header of the original request had the victim's session cookie in it, that session cookie can now be picked off the HTTP TRACE response and sent to the adversary's malicious site. XST becomes relevant when direct access to the session cookie via the document.cookie object is disabled with the use of httpOnly attribute which ensures that the cookie can be transmitted in HTTP requests but cannot be accessed in other ways. Using SSL does not protect against XST. If the system with which the victim is interacting is susceptible to XSS, an adversary can exploit that weakness directly to get his or her malicious script to issue an HTTP TRACE request to the destination system's web server. In the absence of an XSS weakness on the site with which the victim is interacting, an adversary can get the script to come from the site that he controls and get it to execute in the victim's browser (if he can trick the victim's into visiting his malicious website or clicking on the link that he supplies). However, in that case, due to the same origin policy protection mechanism in the browser, the adversary's malicious script cannot directly issue an HTTP TRACE request to the destination system's web server because the malicious script did not originate at that domain. An adversary will then need to find a way to exploit another weakness that would enable him or her to get around the same origin policy protection.

**Resources Required**  
None: No specialized resources are required to execute this type of attack.

**Related Attack Patterns**  
NATURE:ChildOf:CAPEC ID:593NATURE:CanFollow:CAPEC ID:63

**Execution Flow**  
STEP: 1. PHASE: Explore: DESCRIPTION: [Determine if HTTP Trace is enabled] Determine if HTTP Trace is enabled at the web server with which the victim has an active session. TECHNIQUE: An adversary may issue an HTTP Trace request to the target web server and observe if the response arrives with the original request in the body of the response. STEP: 2. PHASE: Experiment: DESCRIPTION: [Identify mechanism to launch HTTP Trace request] The adversary attempts to force the victim to issue an HTTP Trace request to the targeted application. TECHNIQUE: The adversary probes for cross-site scripting vulnerabilities to force the victim into issuing an HTTP Trace request. STEP: 3. PHASE: Exploit: DESCRIPTION: [Create a malicious script that pings the web server with HTTP TRACE request] Create a malicious script that will induce the victim's browser to issue an HTTP TRACE request to the destination system's web server. The script will further intercept the response from the web server, pick up sensitive information out of it, and forward to the site controlled by the adversary. TECHNIQUE: The adversary's malicious script circumvents the httpOnly cookie attribute that prevents from hijacking the victim's session cookie directly using document.cookie and instead leverages the HTTP TRACE to catch this information from the header of the HTTP request once it is echoed back from the web server in the body of the HTTP TRACE response. STEP: 4. PHASE: Exploit: DESCRIPTION: [Execute malicious HTTP Trace launching script] The adversary leverages a vulnerability to force the victim to execute the malicious HTTP Trace launching script.

**Possible Assets Vulnerabilities**  
⚠ Incorrect Use of Privileged APIs  
⚠ Protection Mechanism Failure

### ACTIVITY TIMELINE

- Campus Technology Limited project details updated. 1 month ago
- Campus Technology Limited project details updated. 1 month ago
- Campus Technology Limited project details updated. 1 month ago
- Campus Technology Limited added as new project. 1 month ago
- CTLAdmin is added as project member. 1 month ago

**Figure 5.14: Threat Modelling**

### 5.7.4.3. Risk Assessment

The Web pages allow the user to view the various aspects associated with risks and their relations. This includes; risk name, risk type, risk likelihood, risk impact, risk level, risk status and control measures.

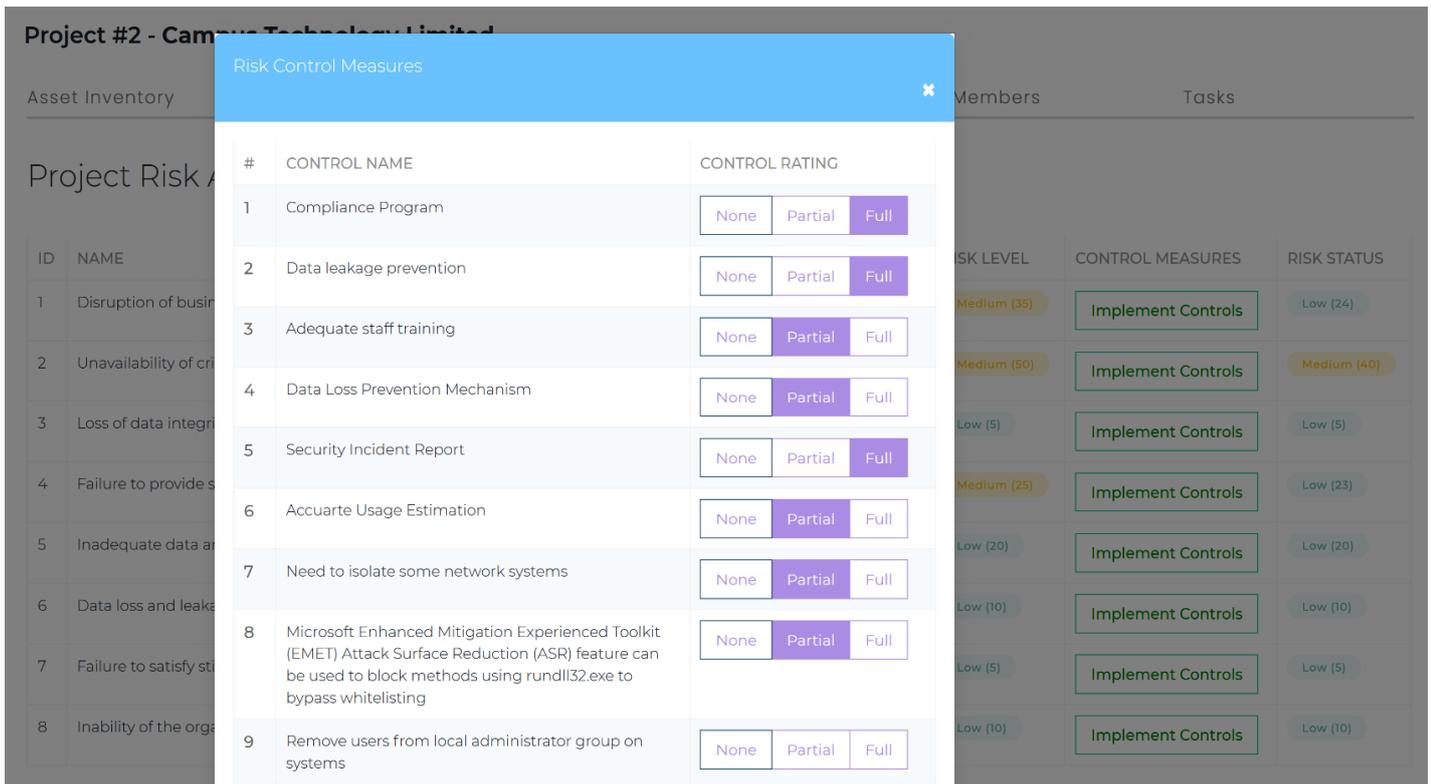
## Project Risk Assessment

ID	NAME	LIKELIHOOD	RISK IMPACT	RISK LEVEL	CONTROL MEASURES	RISK STATUS
1	Disruption of business process	Medium	Risk Impact	Medium (35)	Implement Controls	Low (24)
2	Unavailability of critical data and assets	Medium	Risk Impact	Medium (50)	Implement Controls	Medium (40)
3	Loss of data integrity and unauthorised changes to assets	Medium	Risk Impact	Low (5)	Implement Controls	Low (5)
4	Failure to provide security transparency and accountability by the organisation	Medium	Risk Impact	Medium (25)	Implement Controls	Low (23)
5	Inadequate data and application security, administration and control.	Medium	Risk Impact	Low (20)	Implement Controls	Low (20)
6	Data loss and leakage	Medium	Risk Impact	Low (10)	Implement Controls	Low (10)
7	Failure to satisfy stipulated requirements by the organisation	Medium	Risk Impact	Low (5)	Implement Controls	Low (5)
8	Inability of the organisation to meet compliance needs of data and services	Medium	Risk Impact	Low (10)	Implement Controls	Low (10)

**Figure 5.15: Risk Assessment**

**5.7.4.3.1. Risk Impact rating to determine the risk level**

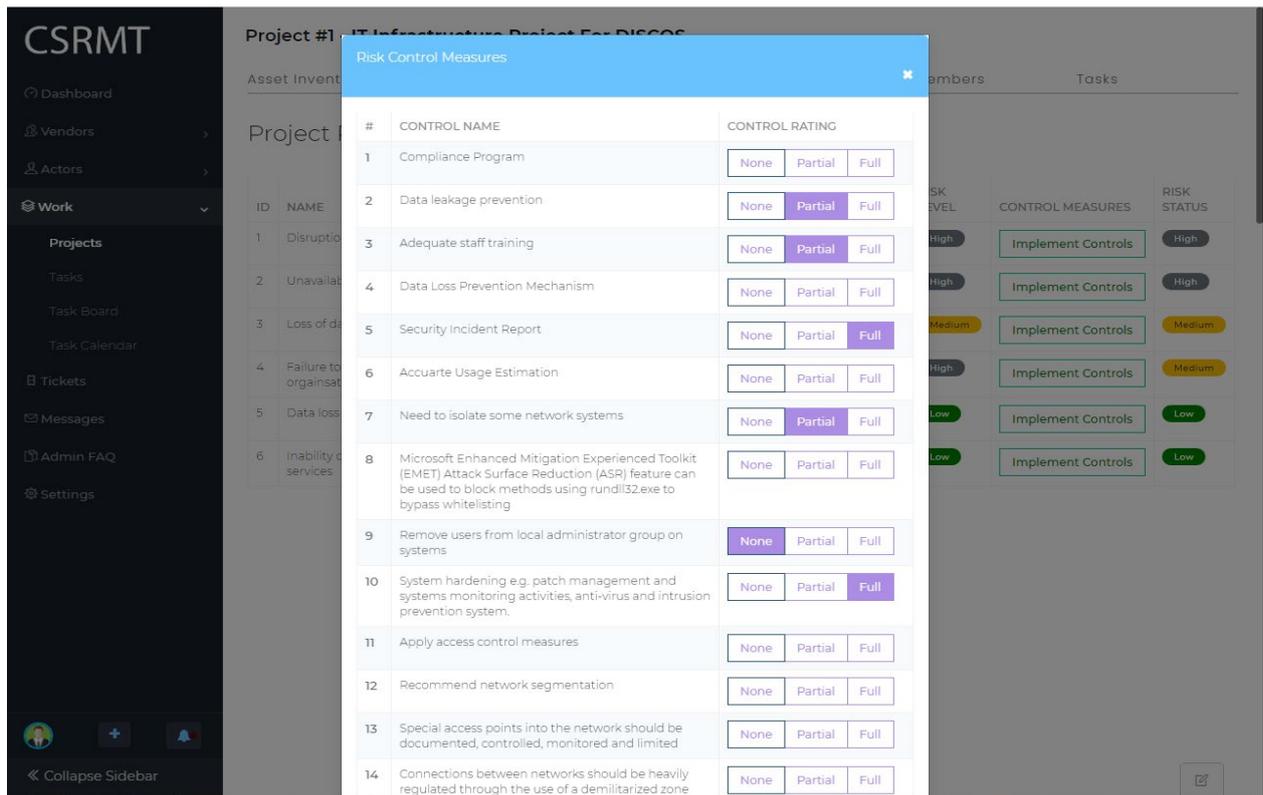
The Web page allows the user to associate the defined risk events with the risk impact factors. This is done by selecting from a simple list of None/Partial/Full questions, which directly impacts the results of the risk calculation for the risk level.



**Figure 5.16: Risk Impact Rating**

**5.7.4.3.2. Select and Implement control measures to reduce the risk level**

The web page presents the risk events and their calculated risk values, and the control measures that can be used to mitigate the risk. To implement the control measures, the users select from a simple list of None/Partial/Full questions, which directly impacts the results of the risk calculation for the overall risk status.



**Figure 5.17:** Implement control measures

#### 5.7.4.4. Evaluate control effectiveness

This page enables the company admin to evaluate the effectiveness of the existing controls. The user can add new controls by selecting a risk name and a control name from the controls list. After that, the user selects; Coverage, Relevance, strength, integration, and traceability as five input ratings for evaluating individual control effectiveness. Each input is assigned five labels; critical, major, moderate, minor and insignificant for assessing the output level. Automatically, the tool returns overall control effectiveness of; critical, major, moderate, minor or insignificant.

**Projects #1 - IT Infrastructure Project For DISCOS**

Asset Inventory Threat Modeling Risk Assessment **Controls Effectiveness** Members Tasks

Controls Effectiveness

[Add New](#)

Risk Name: Disruption of business process Control Name: Remove users from local admini Rating for Relevance: Critical Rating for Strength: Minor

Rating for Coverage: Moderate Rating for Integration: Major Rating for Traceability: Minor

[Save](#)

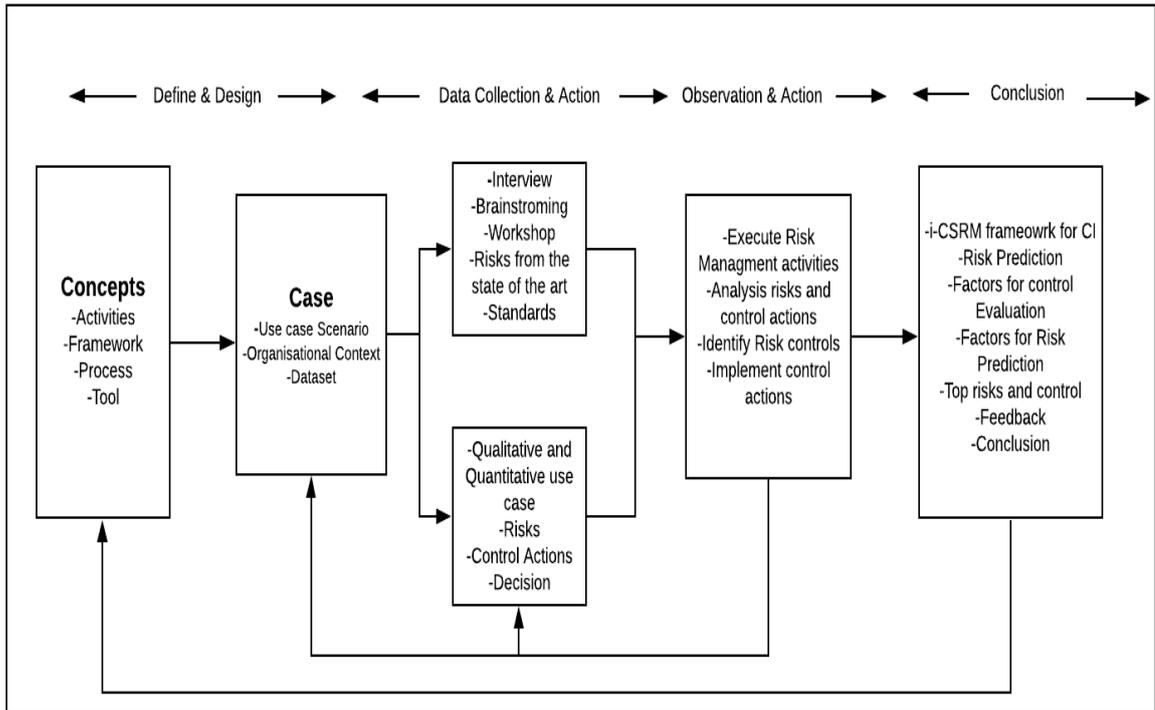
Show 10 entries Search:

ID	RISK NAME	IMPLEMENTED CONTROL	RATING FOR RELEVANCE	RATING FOR STRENGTH	RATING FOR COVERAGE	RATING FOR INTEGRATION	RATING FOR TRACEABILITY	OVERALL CONTROL EFFECTIVENESS
17	Disruption of business process	Remove Users From Local Administrator Group On Systems	CRITICAL (5)	MINOR (2)	MODERATE (3)	MAJOR (4)	MINOR (2)	16 (MAJOR)
Action								
16	Inability of the organisation to meet compliance	Microsoft Enhanced Mitigation Experienced Toolkit (EMET)	MINOR (2)	MODERATE (3)	MINOR (2)	MODERATE (3)	MODERATE (3)	13 (MODERATE)

**Figure 5.18:** Evaluate control effectiveness

## 5.8. Evaluation of i-CSRSM Framework

The i-CSRSM Framework presented in this research is a proposed solution that aims to address the many issues associated with risk management and cybersecurity-related issues. The primary purpose of the evaluation is to determine the applicability of the Framework in a real-world scenario. Evaluation is a principal activity and one of the most critical steps in framework development, especially for a significant importance framework like the i-CSRSM Framework. The evaluation comprises a set of associated methodologies and techniques with a distinct purpose of providing the means to establish the value, quality and relevance of research, and in some cases, provides feedback necessary for improvement (Boudreau, Gefen and Straub, 2001). It also aims to carefully provide a clear-cut assessment for demonstrating the research's ability to produce the desired effect (Straub, Boudreau and Gefen, 2004). There are many empirical evaluation methods and techniques that could be adopted, such as action research, experimental methods and descriptive methods. These methods have been covered carefully in detail in Chapter Three. Figure 5.19 shows an outline of the evaluation approach for the proposed Framework.



**Figure 5.19:** Evaluation Approach for the Proposed Framework

## 5.9. Empirical Research method

We followed an empirical research method through a case study to determine the usefulness of the integrated i-CSR Framework in critical infrastructure. Empirical studies are increasingly becoming popular in information systems research (Runeson and Höst, 2009) because it has proven to be an effective research method to collect relevant data for investigating a specific problem in information systems. Therefore, the case-study approach was employed to serve as the evaluation approach for this research, whereby a company was selected based on accessibility through the researcher's contacts. A case-study approach is widely used in the information systems research domain because it helps explanatory research projects and serves as a basis for developing well-structured research findings (Straub, Boudreau and Gefen, 2004). The case study is an empirical investigation that carries out an existing occurrence within its real-life context. The rationale behind employing a case-study is to obtain meaningful feedback regarding the validity and usefulness of the i-CSR Framework and stakeholders' view on the usefulness of i-CSRMT. Also, the author used questionnaires to collect feedback from stakeholders in the case-study contexts for improving the Framework.

Questionnaires were organised to form the guiding principles for collecting data. In particular, the questionnaire aims to collect stakeholders' perception and view about the use of i-CSR Framework and i-CSRMT in terms of its acceptability and validity, supporting the calculation of an accurate risk

level and overall risk management. The questionnaires contain pre-formulated questions with defined response options. This consideration made the questionnaire highly relevant in obtaining feedback as the questions are designed to help stakeholders express their view. It is imperative to develop the questionnaires using essential criteria formed according to established models for information systems adoption (Thong, 1999). Specifically, these criteria are developed by considering the Unified Theory of user Acceptance of Information Technology (UTAUT) proposed by Davis (Davis, 1989) and the Technology Acceptance Model (TAM) (Venkatesh *et al.*, 2003). The rationale behind these two models is that they are both widely used for assessing the organisation-level adoption of various information systems products and services. Essentially, the criteria included ease of use/clarity, relevance, usefulness, flexibility and dynamics, conformity to security standards and best practices, trustworthiness (as shown in Appendix A).

### 5.9.1. Data collection

At the initial stages of evaluation, opening workshops were organised at the respective studied context. Workshops were attended by senior management representatives and IT personnel with at least three years of working experience. The primary aim was to introduce stakeholders' role in terms of the evaluation exercises and feedback collection through the questionnaire. An overview of the i-CSRMT Framework's process and the essential features of i-CSRMT were introduced to help stakeholders understand how the process/tool works, expected deliverables, procedures, and the methodology involved for data collection. During the workshops, the process and evaluation activities for the i-CSRMT Framework and briefing on how to use i-CSRMT and its features were the main point of the presentation in the case study. Further briefing on how the risk type prediction is carried out using machine learning on the VCDB dataset is explained.

Therefore, a total of 50 versions of the questionnaires were distributed across the organisation. The project aimed to introduce how their feedback can contribute towards validating i-CSRMT framework/i-CSRMT, risk prediction, and the overall research findings. They were briefed about the criteria followed in formulating the questionnaire. Besides, the possible responses are designed to fit the purpose and can be indicated as either "I strongly agree", "I agree", "Not sure", or "Disagree".

Overall, stakeholders from the case-study context returned a total of 40 questionnaires, implying a response rate of 80%. Table 5.1 provides a summary of the stakeholders that were involved and responses to the questionnaire within the studied case study.

**Table 5.1:** Summary of Responses from researched case-study

Case Study	Participants		Respondents	
	Senior Management	IT Staff	Senior Management	IT Staff
Case Study	15	35	12	28

Total	50	40
-------	----	----

### 5.10. Dataset Description: Implementation of Machine learning classifiers for Risk prediction

We used the dataset from "Veris Community Database (VCDB)" (Widup, 2013), which aims to collect and disseminate data breach information for all publicly disclosed data breaches, to test our classifiers. It provides some of the enormous available collection of datasets that consists of collective intelligence report dataset allowing us to test the classifiers' performance in predicting risk type. We further created a mapped version of this dataset by selecting some features in the dataset and mapping them to TTP, Threat Actor, Asset and Control categories. For example, brute force is mapped to TTP. We extracted the features in VCDB that are of interest in training and testing our classifiers. Based on the requirements we used exploratory data analysis (EDA) process to clean the data. EDA is a step in data analysis process where a number of techniques are used to better understand the dataset being used by; extracting important variables and removing all the null values and features with null values. For example; Assets type, we looked at the types of compromised assets during the incident, Actor type and motive; we train our classifiers based on the actor responsible for the incident. We used the final mapped dataset to build out model over it. The full features are 512 and the sample size is 7,834.

In (Liu, Sarabi, et al., 2015), data on reported cybersecurity incidents are needed to serve as ground-truth for their study. Such data is required to train the classifiers as well as assess their accuracy in predicting incidents. VCDB is used to train and test a sequence of classifiers/predictors. Therefore data from the VCDB is collected to obtain proper coverage.

#### 5.10.1. Mapping

In this section, we explain the mapping of the existing dataset features to our proposed i-CSR framework concepts and then applied ML on the mapped dataset. The data for each i-CSR feature is mapped to the VCDB dataset as shown below:

- **Discovery and Response:** This entry in the VCDB dataset is our Control feature. It focuses on the timeline of the events and how the incident was discovered. It provides valuable insights into the organisation's detection and defensive capabilities and helps identify corrective actions needed to detect or prevent similar incidents from occurring.
- **Incident Description:** this entry is mapped to our Threat Actor, TTP and Assets features. It focuses on "whose actions affected the assets", what actions affected the assets", and which assets were affected". Threat Action (TTP) describes what the Threat Actor did to cause or contributes to the incident, such as Malware, Hacking and Misuse. Actors (Threat Actors) are entities that cause or contribute to any particular incident, and their actions can be malicious, intentional or unintentional. Threat Actors are recognised in VCDB as external, internal and

Partner. Assets (Assets) describe the information assets that were compromised during an incident. Compromised means the loss of confidentiality, integrity, availability and authenticity. Assets are categorised into Variety (such as SCADA), Ownership, Management, Hosting, Accessibility and Cloud.

The features extracted from VCDB are used for training and testing our classifiers. Details documented in the dataset include the TTP used, assets compromised, threat actor type and motive and controls. The list of features extracted from the VCDB dataset that are mapped to CSRM concepts is shown in Tables 5.2, 5.3, 5.4 and 5.5.

- **Threat Actor:** The first set of Mapping is information regarding the individual, group of individuals or organisations that are believed to have operated with malicious intent. Therefore, each incident is put in one of the four categories: External, internal, Partner and unknown threat actor types. Each category includes additional features that further differentiate the threat actor type. For instance, an external threat actor is further categorised as organised crime, former employee, competitor, espionage and grudge. The Partner is further categorised as the industry. The internal threat actor is categorised as hired, demoted, personal issues, resigned, auditor, cashier and developer. Therefore, we train our classifiers based on the threat actor responsible for the incident. Predicting risk requires information about the threat actor type and motive; this allows organisations to determine the policies to educate their employees, access their data, safeguard their networks from attackers and perform due diligence when selecting partners as the third party.

**Table 5.2:** Feature vector for threat actor for VCDB dataset

<b>Threat Actor Type</b>	Espionage	Competitor	Grudge	System Admin	Financial	Fun	End-User	.....	Developer
<b>Number of features</b>	1	2	3	4	5	6	7	.....	80
<b>Total Number of Data points</b>	7,834								

- **Assets:** Mapping is done for the assets that were compromised during the incident of the attack. There are six categories of asset types: server, media, user device, terminal, people and networks. Knowing the type of assets that are more likely to be affected can significantly improve their ability to predict risk following security incidents. Organisations can further implement

appropriate controls, such as network administrators keeping regular backups on media and server assets.

**Table 5.3:** Feature vector for the asset for VCDB dataset

Asset Type	Disk drive	Documents	Access reader	LAN	Router/Switch	Patch Management	RTU	.....	Database
Number of features	1	2	3	4	5	6	7	.....	234
Total Number of Data points	7,834								

- **TTP:** This set of Mapping is information regarding the type of attack, based on which each TTP can be put in one of seven general categories: Environmental, error, hacking, malware, misuse, physical and social. Each category of TTP includes additional features that can help to differentiate incidents further. For instance, SQL injection and brute force are identified as hacking. Hacking incidents involve data breach through compromised credentials. Physical incidents include theft leading to tampering. Knowing the TTP type can provide organisations with valuable information on preventive measures to reduce risk. Secure passwords, setting and enforcing internal regulations and avoiding unnecessary access privileges for employees can be used to prevent hacking incidents.

**Table 5.4:** Feature vector TTP for VCDB dataset

TTP Type	Remote access	Ransomware	Remote injection	SQL injection	Spyware/keylogger	Brute force	Buffer overflow	...	E-mail attachment
Number of features	1	2	3	4	5	6	7	...	155
Total Number of Data points	7,834								

- **Controls:** The control types fall into one of the two categories detective and corrective controls. We train our classifiers based on the controls available at the time of the attack. We further categorise Detective into sub-categories: Internal (log review, antivirus, data loss prevention, fraud detection) and external (actor disclose, incident response, monitoring service, suspicious traffic). Assessing the risk associated with controls prompts organisations further to determine the set of security protections or countermeasures to minimise risk. Some of the controls might be

insufficient to mitigate risk, so these different control types that were compromised at the time of the attack are the properties that serve as features for machine learning classifiers to predict risk type and appropriate controls implemented.

**Table 5.5:** Feature vector for control for VCDB dataset

Control Type	Fraud detection	Incident response	Monitoring service	Antivirus	IT Review	Log Review	Security alarm	.....	Law enforcement
Number of features	1	2	3	4	5	6	7	....	42
Total Number of Data points	7,834								

- **Full:** The full feature is a combination of all the other four features (Assets, Controls, Threat Actor and TTP). The full feature contains a total number of 512 features and a total of 7,834 data points.

### 5.10.2. Experimental Setup

Our experiments used VCDB dataset because it has been used in literature providing easier benchmarking, and we have feature information about cybersecurity. Further, in our experiments, we used Jupyter notebook and python 3.6 interpreters to run our codes. The dataset is divided into 80% of the samples for building the model and the remaining 20% for testing.

### 5.10.3. Feature Extraction

Feature extraction is the first step to start a machine learning process because it is a technique that aims at finding specific pieces of data in natural language and then converts them into a suitable format for machine learning classifiers to train. Our research draws from various data sources that collectively characterise the security posture of organisations and the security incident report used to determine their security outcomes. In this step, we extract all the necessary features from the dataset to map the i-CSRSM concepts presented in chapter three. Every concept has properties, and those properties are considered as features, for example:

- Asset concept features include; Server, media, people, networks, user device and terminal.
- Threat actor features include; External, Internal and supply chain partner.
- Control features include; corrective, Detective and preventive.

- TTP features include; Malware, hacking, social, physical, environmental, misuse and error.

The features are further converted into a format suitable for the machine learning classifiers by assigning a weight between 1 and 0.

#### 5.10.4. Features and classification labels

This section presents the data type values used in the experiments and includes a list of features extracted from the dataset. The reason for choosing these feature types is because they are salient, straightforward and intuitive, and any machine learning classifier can be trained over them. Asset, threat actor and controls are assigned binary numerical data type and given a possible value between 0 and 1. It consists of two sub-steps.

##### 5.10.4.1. Features weights and labels

Dataset is collected from the "Veris Community Database (VCDB)" (Widup, 2013). We then mapped the features in the dataset to i-CSRMs concepts, which are used as features for the Classification and assigned their weights. We used feature extraction techniques coupled with human annotation for extracting the essential features from the dataset. The risk type is the output class we are predicting, and the ordinal categorical data type is used with possible values from 1 to 10 (Refer to Table 5.13).

#### Output Feature

We have used ten output categories of risks, and the value range for the features is from ( $R_1 =$  Crimeware,  $R_2 =$  Cyber espionage,  $R_3 =$  Denial of service,  $R_4 =$  Everything else,  $R_5 =$  lost and stolen assets,  $R_6 =$  miscellaneous errors,  $R_7 =$  payment card skimmers,  $R_8 =$  point of sale,  $R_9 =$  privilege misuse and  $R_{10} =$  web applications) with possible classes. This is a multi-class problem, and we have the following risk types as output features explained in Table 5.6. The input features are shown in Tables 5.7, 5.8, 5.9 and 5.10. These features are used to categorise the input features (threat actor, control, assets and TTP) into ten categories. The classification model is trained on the following categories listed in the Table 5.6.

**Table 5.6:** Feature vector as output features for control for VCDB dataset

Feature name	Possible classes	Range of values
Crimeware	$R = \{R_1, R_2, R_3 \dots R_{10}\}$	$\{1,2,\dots,10\}$
Cyber Espionage	Where:	
Denial of Service	$R_1 =$ Crimeware	
Everything Else	$R_2 =$ Cyber Espionage	
Lost and Stolen Assets	$R_3 =$ Denial of Service	
Miscellaneous Errors	$R_4 =$ Everything Else	

Payment Card Skimmers	$R_5$ = Lost and Stolen Assets	
Point of Sale	$R_6$ = Miscellaneous Errors	
Privilege Misuse	$R_7$ = Payment Card Skimmers	
Web Applications	$R_8$ = Point of Sale	
	$R_9$ = Privilege Misuse	
	$R_{10}$ = Web Applications	

### Input features

We consider different classes of input feature such as threat actor (t), asset (A), TTP (TTP), and control (C). Table 5.7 shows the threat actor feature types with possible classes  $\{t_1, t_2, t_3\}$ , representing the different threat actor feature types. They are trained on the proposed classifiers, and the possible values are between  $\{0, 1\}$ .

**Table 5.7:** Threat Actor type feature detail

Feature name	Possible classes	Range of values
External	$t = \{t_1, t_2, t_3\}$	$\{0, 1\}$
Internal	Where:	
Supply chain Partner	$t_1$ = External	
	$t_2$ = Internal	
	$t_3$ = Partner	

Table 5.8 shows the different asset feature types used as an input parameter for risk type prediction. The asset (A) features are given as  $\{A_1, A_2 \dots A_6\}$  representing the different asset types and are trained on the proposed classifiers. The possible values are between  $\{0, 1\}$ .

**Table 5.8.** Asset type feature detail

Feature name	Possible classes	Range values
Server	$A = \{A_1, A_2 \dots A_6\}$	$\{0, 1\}$
Terminal		
Media		
People		
Networks		
User device		

Table 5.9 below shows the control (C) feature types that are used as input parameters for predicting risk type. They include  $\{c_1, c_2, c_3\}$  representing the different types of control types with possible values between  $\{0, 1\}$ .

**Table 5.9.** Control type feature detail

Feature name	Possible classes	Range of values
Detective Corrective Preventive	$C = \{c_1, c_2, c_3\}$ Where: $c_1 =$ Detective $c_2 =$ Corrective $c_3 =$ Preventive	{0, 1}

Table 5.10 shows the different TTP feature types used as input features trained on the proposed classifiers. They are given possible values as {TTP1, TTP2....TTP7} represent the different TTP feature names and are given possible values between{0, 1}.

**Table 5.10:** TTP type feature detail

Feature name	Possible classes	Range of values
Malware Hacking Social Physical Misuse Error Environmental	$TTP = \{TTP_1, TTP_2, \dots, TTP_7\}$	{0, 1}

#### 5.10.4.2. Assigning Weights to Feature Vectors

The full vector takes the whole dataset into account. We used the binary values of either 0 or 1 {0, 1} to the feature vector, as shown in Table 5.11.

**Table 5.11:** Feature vector weights

Feature Vector	Feature vector Weights
TTP Control TA Asset Full	$V_B \in \{0, 1\}$ For a given feature vector ' $F'$ ', the value ' $v'$ ', of any feature ' $x'$ ' is determined using the following rule: $v_B^x = \left\{ \begin{array}{l} 1, \text{if occur} \\ 0, \text{otherwise} \end{array} \right\}$ The output value for any feature is {1} if the corresponding feature occurs in the dataset. Otherwise, its value is recorded {0}

### 5.10.5. Classification

Classification is an essential step for machine learning to understand and assign data categories for accurate risk prediction. Once we have extracted all the features, the next step is to classify the features. To achieve the Classification, we follow seven different algorithms to generalise our findings of integrating machine learning with i-CSRMs to predict a particular risk type. The classifiers calculate both the likelihood and impact and find complex relationships in data to produce better results than the rest. Once the feature weights are defined, we train the machine learning classifiers over the training data. For the given partition and classifier, the results are shown using the following notation: (refer to Table 5.12)

**Table 5.12:** Classification Models and feature description

Scenarios	Assets	Controls	Threat actor	TTP	Models
$Set_B$ PCA is not applied	$Asset_B \in \{0, 1\}$	$Control_B \in \{0, 1\}$	$TA_B \in \{0, 1\}$	$TTP_B \in \{0, 1\}$	$Model_{Set_B}^{Classifier}$ where $Set_B \in \{Assets, Controls, Threat\ actor, TTP\}$
$Set_{PCA_B}$ PCA is applied	$Asset_{PCA_B} \in \{0, 1\}$	$Control_{PCA_B} \in \{0, 1\}$	$TA_{PCA_B} \in \{0, 1\}$	$TTP_{PCA_B} \in \{0, 1\}$	$Model_{Set_{PCA_B}}^{Classifier}$ where $Set_{PCA_B} \in \{Assets, Controls, Threat\ actor, TTP\}$

We used the notation,  $Set_{PCA}$  to denote the feature sets that have been reduced by applying PCA. For example, the feature vector control is denoted by  $Control_B$  moreover, in case this feature vector has been transformed by PCA; we denote it by  $Control_{PCA_B}$ . Similarly, the model built over feature set transformed by PCA is denoted by  $Model_{Set_{PCA}}^{Classifier}$ .

PCA is a dimensionality reduction algorithm where new features are created which represents the original feature dimensions in a lower dimension with a little loss of the total information. PCA reduces the dimensionality by projecting high dimensional data along a smaller number of orthogonal dimensions. We use PCA because there are a lot of features and certain features might not be visible when we use them in the same manner. Therefore, we use PCA for selecting the most relevant features such as Assets and TTP. There might be some hidden information between features. Like TTP and controls might be linked to each other which we can't see in the high level scenario. PCA try to find some hidden relation between the features and it helps to remove noise and increase

dimensionality and scalability of the data. This is a well known approach in literature used for reducing noise.

### 5.10.6. Training the machine learning classifiers

This section describes the training of machine learning classifiers using training data. We use extracted features enclosed in the training examples to find a model  $M: D \rightarrow R$ , which approximates  $T$ . The function  $R$  defines the class to which the learned model assigns the given sample  $d$  and is used to classify new scenarios. The model  $M(d)$  denotes a machine learning classifier. The objective here is to find a model that maximises accuracy (assigns a scenario to the most proper class).

**Table 5.13:** Notations used for building the classifier

Notation	Description
$D$	The collection of cyber-attack scenarios
$d' = \{d_1, d_2, \dots, d_N\}$	N number of scenarios to be classified
$R = \{R_1, R_2, R_3, R_4, R_5 \dots R_{10}\}$	R is the number of possible risks categories
$d' = \{d_1, d_2, \dots, d_N\}$	The training set consisting of N scenarios with corresponding actual class labels $y = R = \{R_1, \dots, R_{10}\}$
$T$	A target concept $T: D \rightarrow R$ , which maps given a scenario to a class (we assume the categories are disjoint, i.e. each given scenario can only be categorised into one of the categories, and there is no overlapping between categories)
$M: D \rightarrow R$	A machine learning model, which approximates T (i.e. close to T)
$M(d)$	The model prediction for unknown scenario 'd' (i.e. the model predict using a classification algorithm, which classes the unknown scenario belongs to)

The Accuracy matrix can be formally defined as:

$$\text{Accuracy} = \frac{\sum_{x \in d'} \mathbf{1}_{M(d)=R_d}}{|d'|} \quad (\text{Equation 5.1})$$

Where  $|d'|$  is the size of the test set (number of scenarios to be classified), and  $1_{M(d)=R_d}$  It is an indicator function that output one if the model predicted the class for the test scenario is the same as the actual test class and zero otherwise. Formally:

$$1_{M(x)=R_x} = \begin{cases} \mathbf{One} & \text{if } M(x) = R_x \\ \mathbf{0} & \text{otherwise} \end{cases} \quad (\text{Equation 5.2})$$

The proper controls also increase the accuracy score, which corresponds to a classification error's low rate.

### 5.10.7. Evaluation measures

Some of the standard measurements used to evaluate information retrieval information methods are Precision, Recall and F-1. Therefore, this section presents Precision, Recall and F-measure as evaluation measures. These metrics are used to validate accuracy in different ways, yet they can be applied to other purposes and describe how risk prediction methods are successful.

The precision gives us the probability that a selected value is true. It can be formally defined as:

$$\textit{Precision} = \frac{\textit{True Positive}}{\textit{Total predicted positive}} \quad (\text{Equation 5.3})$$

The Recall gives us the probability that the true value is selected. It can be formally defined as:

$$\textit{Recall} = \frac{\textit{True Positive}}{\textit{Total Actual Positive}} \quad (\text{Equation 5.4})$$

The F1 Score is a function of the Precision and Recall and can be formally defined as:

$$F1 = 2 * \frac{\textit{Precision} * \textit{Recall}}{\textit{Precision} + \textit{Recall}} \quad (\text{Equation 5.5})$$

## 5.11. Case study: Implementation of i-CSRМ Framework

This presents the implementation of the i-CSRМ framework process as well as i-CSRMT using the case-study. By following the i-CSRМ process from start to end over some time, we systematically applied all the activities and steps within the i-CSRМ process using i-CSRMT and the opportunity to collect feedback towards evaluating its validity. Therefore, a detailed description of the case study is provided by first presenting background information and implementing the existing system. This is concluded by a practical demonstration of how the i-CSRМ Framework was achieved.

### 5.11.1. Study context

DisCos power holding company in Nigeria distributes electricity (Kemabonta and Kabalan, 2018) across the country, which serves at least 30,000 customers within a geographical area, with several branches and employees located in different states Nigeria. The company is structured based on

functional divisions, which include administration, support and IT. The company's first services are to provide last-mile services in the electricity supply value chain, transforming or stepping down electricity from the high voltage at the transmission level to lower voltage depending on the customer's category. They are responsible for the marketing and sale of electricity to customers, providing a tax to the government, collecting bills, handling electronic payments, exchanging information and providing customer care functions in its geographical area. In improving the continuity of service, timely recognition of faults, continuous monitoring and protection of the power systems, the company recently implemented a supervisory control system in all of its branches for sustainable service delivery.

### **5.11.2. The Workflow**

The power distribution happens through a power distribution substation that comprises other components such as circuit transformers, breakers, and a bus bar. The transformers increase (step-up) or reduce (step down) voltages to adjust to the different stages of the journey from the power plant on long-distance transmission lines to distribution lines that carry electricity to homes and businesses. Circuit breakers enable the disconnection of distribution lines during maintenance or upgrade and isolating faults in the distribution lines. The bus bar splits and distributes power to distribution lines for reaching out to customers. The substation's whole distribution process and components are managed by a cyber-physical control system, consisting of a Supervisory Control and Data Acquisition (SCADA) system. In other words, the SCADA system monitors the entire power control system in real-time by performing automatic monitoring and controlling of various equipment within the distribution lines. It also maintains the desired operation conditions, interrupts and restores power service during fault conditions. SCADA system also checks the status of various equipment continuously and sends control signals to the remote control unit accordingly. Further, it also performs operations such as bus voltage control, load balancing, circulating current control, overload control, and transformer fault protection

### **5.11.3. Recent Cyber Incident**

DisCos is an official body with branches geographically split (Onochie, Egware and Eyakwanor, 2015); each has its workstations networked to allow personnel to perform their tasks. All branches deployed a new SCADA system to improve power reliability, cybersecurity, and resilience to disruption. They use a SCADA consisting of 5 generic machine types connected to a local Ethernet LAN to support their services. In a recent event, an employee monitoring the SCADA system in one of the branches received a carefully crafted spear-phishing e-mail message from a highly skilled anonymous organisation that contained a malicious Microsoft Word attachment and disguised as a medical report of his sick son. The employee clicked and opened the document, and malware was discovered to have spread across the network, operating systems, and targeting the SCADA system,

which led to the unstable power system operation in the branch. The anonymous organisation gathered hashed credentials over a server message block (SMB) to identify information by downloading the word document. The anonymous organisation accessed workstations and servers on the corporate network that contained data output from control systems, accessed files about the SCADA systems, leaked network credentials, organisational design and control system information to a command and control server outside DisCos organisation, and accessed e-mail accounts using outlook web access (OWA).

The anonymous organisation used a virtual private network (VPN) to maintain access to networks even with network proxies, gateways and firewalls. After the employee visited one of the compromised servers, a backdoor was installed on the machine, providing the anonymous organisation with remote access to the environment (networks, systems, databases). The anonymous organisation having available resources, disabled the host-based firewalls, obtained a foothold and the exploration activity primarily centred on identifying the central host computer server with the highest volume of personally identifiable information (PII) script folder and file names from hosts. The anonymous organisation gained access to the database host computer server by leveraging its active directory information to identify database administrators and their computers. Passwords were cracked using password-cracking techniques, allowing the anonymous organisation to gain full access to those systems. This caused a loss of data and operational disruption as a result of network and computer security failure. This particular incident has resulted in an electrical power blackout that remained for up to 2 weeks, affecting around 30,000 customers and their businesses. As a result, DisCos has decided to use i-CSRМ framework to assess future impact and control measures for similar incidents in the other branches. A brief description of a scenario allows us to exemplify how the DisCos could benefit from our proposed Framework.

### **5.12. Implementation of i-CSRМ for the Study Context**

As DisCos is considering applying the i-CSRМ Framework and the use of i-CSRMT, we had the opportunity to determine its relevance to a real-life context. As part of managing the entire evaluation process, the company assigned a team of professional stakeholders to guide the entire evaluation process and ensure necessary support to ensure evaluation is achieved in an ideal manner. This section provides a detailed description of how i-CSRМ and i-CSRMT were applied to the case study.

Before starting the activities, a meeting was organised where the evaluation plan's overall setting was decided, a project team was developed, and a first step is taken towards starting the activities. The project team comprises representatives from senior management, the IT department and other stakeholders within the company. The project leader starts the meeting by giving a brief presentation of the i-CSRМ Framework and i-CSRMT, its aim, what the company can expect from the

implementation, and the role of participants, data collection, and a proposed meeting plan. The project leader also reminded the organisation of the responsibilities concerning providing necessary information and documentation about the assets, threat intelligence report and background, business process, and allocating human resources with suitable expertise to participate in the evaluation process. Hence, the implementation process was performed through organised meetings, workshops, and discussions presented below.

### 5.12.1. Activity 1: Organisational Context

Through senior management support and active involvement, we embarked upon initial knowledge extraction and organisational context discovery activity to gather initial information that facilitated identifying the company’s business strategy. We started the activities defined in the proposed i-CSR Framework with the organisational context, which allowed us to identify the organisation’s key objectives and understand the key actors and their roles within the organisation. This enabled us to interact more effectively with key actors to gather information and implement the proposed i-CSR Framework. By conducting the organisational context analysis activity, we were also able to identify and prevent potential misconceptions about each stakeholder’s position and roles and identify sources of information regarding the organisation.

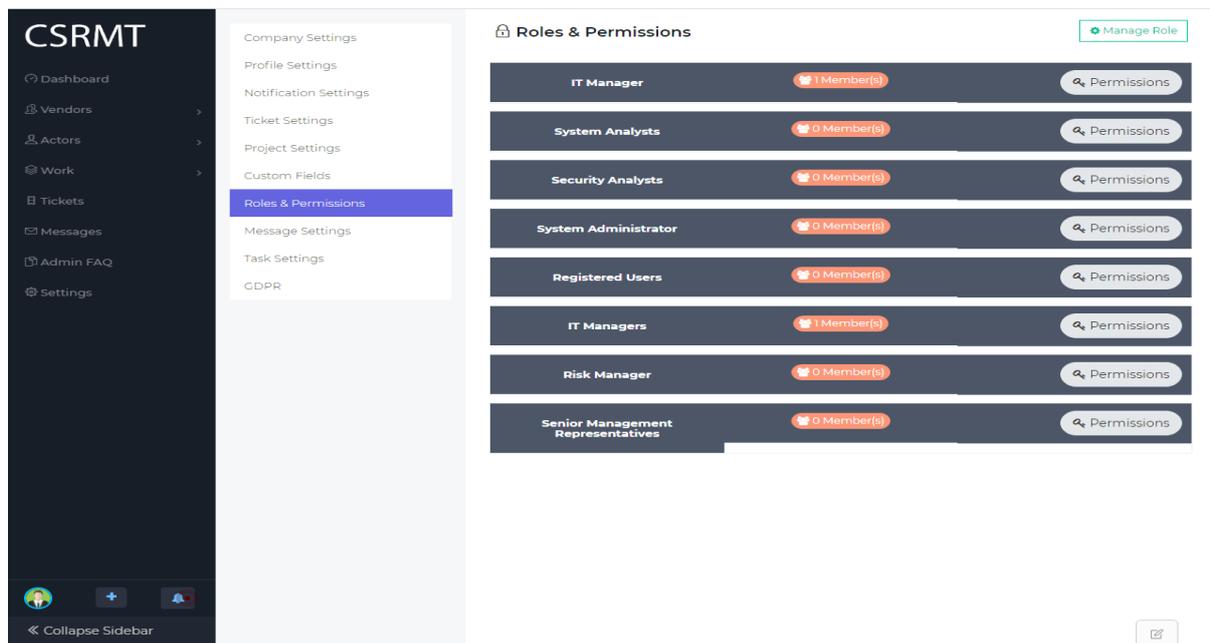
#### 5.12.1.1. Step 1: Identification of Actors and their roles

During the initial meeting and interaction with the implementation team, we were able to identify the key actors that support and influence the project and the different roles they play within the organisation. This enabled us to interact more effectively with the key actors to gather information and implement the proposed i-CSR Framework. Also, we considered actors from within and outside the organisation, which were categorised into internal and external actors. To present a comprehensive picture of actors, we have created an actor list showing actors and their roles. Each actor has a certain degree of activeness. Some actors fully participated in the CSR implementation, while other actors were passive. Table 5.14 provides a list of different actors and their roles. Using i-CSRMT, an organisation can set each actor with their respective roles and define the permission associated with that role. When you create the role, you can assign an employee associated with that role, as shown in Figure 5.20 and 5.21.

**Table 5.14:** List of Actors and their Roles

Type	Actors	Role
Internal	Senior Management representatives	Comprises high ranking personnel of the company whose responsibility is to coordinate, plan, oversee and direct the overall project.
	IT Managers	In charge of the company’s technology strategy and responsible for coordinating and leading the

		company's IT experts/IT department in implementing the Framework's process.
	System Analyst	Responsible for coordinating the development of systems, asset requirements, and control measures for ensuring the security of all assets.
	System Administrator	Responsible for the technical oversight of the entire content management system. He was also charged with installing, supporting and maintaining servers, responding to service outages and other problems.
	Security Analyst	Responsible for identifying cyber threats and establishing plans and controls to protect assets. Also responsible for performing vulnerability testing, risk analysis and security assessment activities
	Risk Manager	Risk Manager communicates risk policies and processes for an organisation. They ensure controls are operating effectively, provide hands-on development of risk models involving market, credit and operational risk and provide research and analytical support.
	Registered Users	Registered users who have permission to use the system



**Figure 5.20:** Roles of Actors and permission

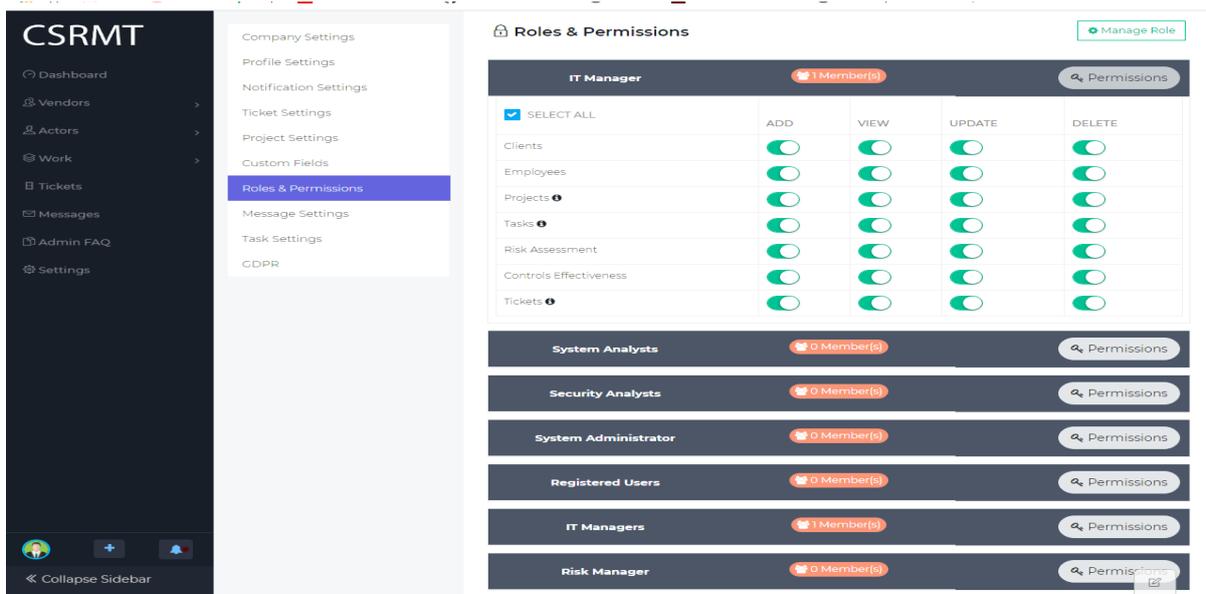


Figure 5.21: Set Actors permission

### 5.12.2. Activity 2: Asset Identification and Criticality

The project team embarked upon initial knowledge extraction through senior management support, and active involvements were initial information that facilitated the identification of the organisation's critical assets. This enabled us to understand how things are done in the organisation regarding its activities, followed by identifying the security goals that are part of an essential component of the organisation's assets and identifying the most critical assets. During this time, the key assets' present architecture was reviewed, the architectural components are identified, and the high-level dependencies between the assets were established. Based on the knowledge acquired, we established asset types, dependency, security goals, and criticality.

#### 5.12.2.1. Step 1: Asset Profile

The IT manager was involved in explaining and documenting the system and its components, which provided the basis to identify the organisation's critical assets and their security, needs to create a consistent asset profile. The IT manager also presented a comprehensive overview of the organisation's assets which are the target of analysis, from where we observed that the system comprises many different components. Based on these discussions, we analysed the system's architecture to establish asset profiles, identify the critical asset, asset dependencies, and interdependencies, including how information is stored and processed. This enabled us to identify critical assets, including data and applications and the security goals that are essential components of the organisation's assets.

During this time, the present architecture of software systems and applications were reviewed, the architectural components are identified, and the high-level dependencies between them were established. We considered factors that influence operations, such as the organisation's structure and the system and processes by which work is carried out. The asset profile is crucial because it can be utilised when developing and applying protection strategy and risk mitigation plans for the system. We prepared an initial asset inventory together with details of the assets as shown in Table 5.15.

**Table 5.15: Assets Identification**

Asset Category	Sub-Asset category
Software assets	Microsoft office
	Master boot record/files
	Mail server
	Service Manager
	Windows/Android operating systems
	UPS remote management interface
	Computer security protection
	Virtual machines
	User identity access management
Hardware assets	Computer systems
	Remote login systems
	Windows machines
	Keystroke Logger
	Hard drives
Data assets	Skype messages
	Internal domain names
	Network/system information
	Sensitive information
	Admin credentials
SCADA systems	Industrial control systems (ICS)
	HMI computers
	Remote terminal unit (RTU)
	Substations
	ICS providers
	SCADA database software
	Programmable logic controllers (PLC)
	Firmware
	Substations Ethernet devices
	SCADA database software
	Workstation
	ICS software application and windows
Information and Communication Networks	Company's computer network
	Virtual private network
	Router/modem/ switches/proxy/gateways
	Firewalls
	UPS server
	Network Internal server
	Public-facing services
	Command and control servers
	Website
	Remote access services
	Operational network
	Remote access services
	URL

	Bluetooth
	Internet service providers

### 5.12.2.2. Step 2: Identify Asset Security Goals

After the asset inventory has been agreed and completed by the team, the next step is to identify each asset's goals. Measuring an asset's goals value requires that numerous factors are considered by using several criteria (Izuakor and White, 2016), such as economic impacts, financial impact, operational impact etc. The security analyst conducted a high-level brainstorming exercise and other team members to identify the most critical security goals for the assets identified in the previous step. At first, some representatives of DisCos emphasised that they are particularly worried about the privacy of data held by the CPS and availability of the services. However, the security analyst explained that the team had reviewed the information collected during the previous step and examined every functional requirement for the system through less important security goals such as confidentiality, integrity, and availability.

The security goals represent factors against which asset criticality is measured and distinguish those assets whose loss could significantly impact the objectives of the critical infrastructure. Hence, after some discussion, the project team decides that the focus of security goals is based on the system's known characteristics and the attributes of security goals should include confidentiality, integrity, availability, conformance, and accountability.

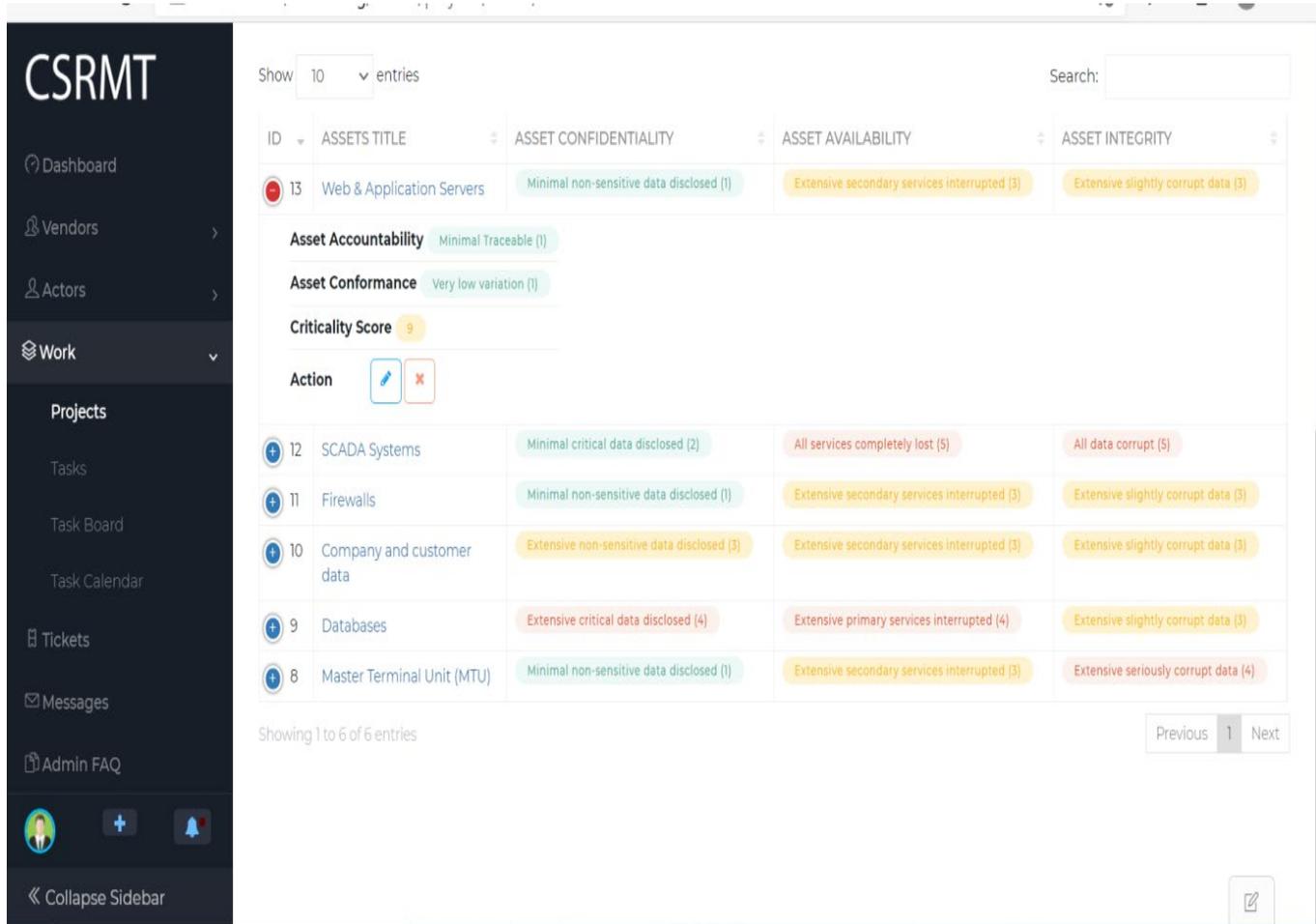
- **Confidentiality:** confidentiality goals are intended to ensure that unauthorised access to data, application and other assets is not permitted, and that accidental disclosure is impossible. Information or data on all the system's components should be restricted to only those with the permission to access.
- **Integrity:** This asset goal ensures that data and applications of the CPS are safe from unauthorised modification and can be modified only by authorised users. It also ensures the accuracy and completeness of records, and only authorised users should be allowed to modify contents.
- **Availability:** Data and resources must be made available for authorised use without interference or obstruction. Data, application, and other system resources must be available when requested and easily accessible to authorised users only.
- **Accountability:** The ability to trace activities or operations that occurred on data, applications or system components to a particular source. All users must be accountable for the operations they perform.

- **Conformance:** CPS must operate as intended without variation to expected behaviour, functions and regulatory requirements. The system must also be secured from vulnerabilities that can be exploited to cause unwanted behaviour.

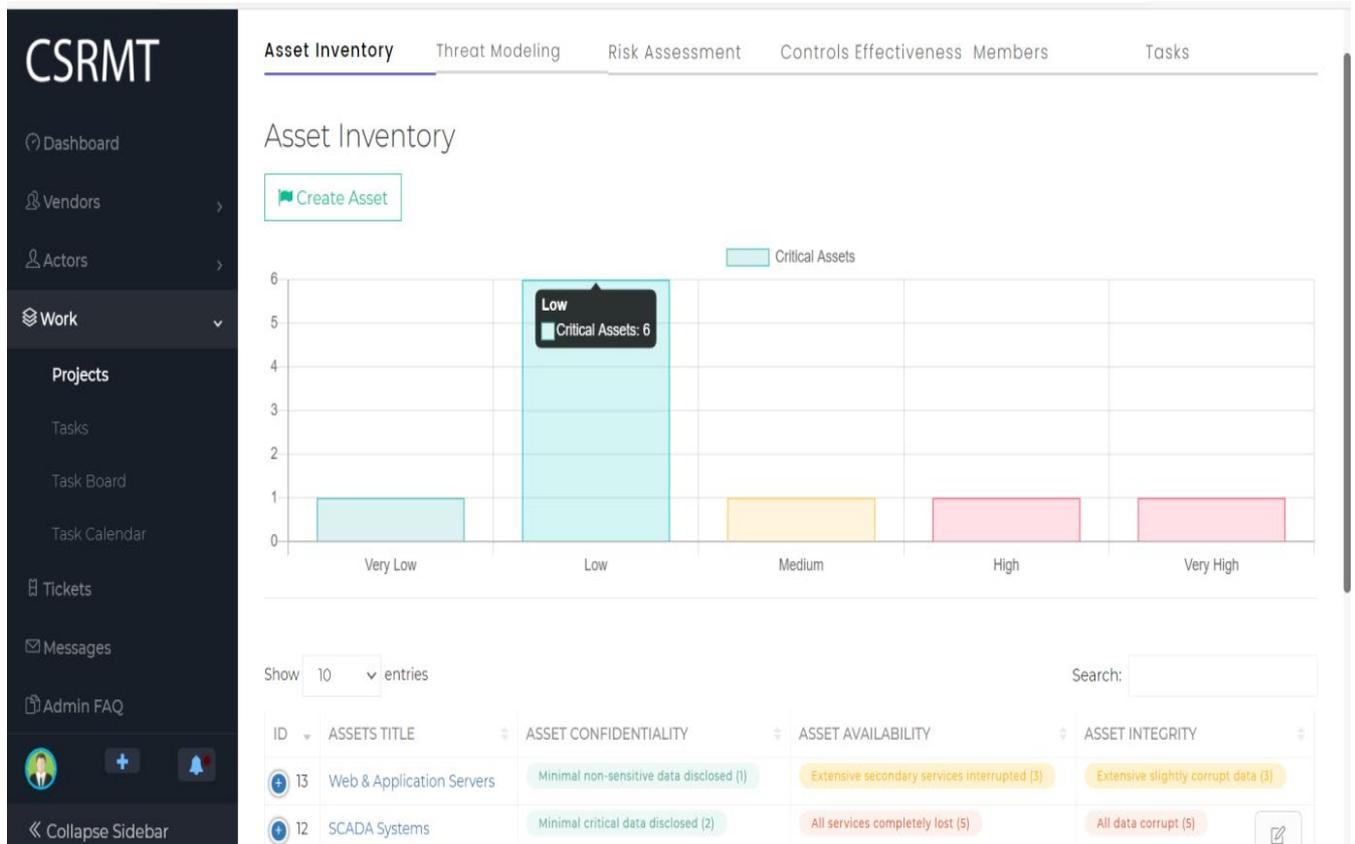
### 5.12.2.3. Step 3: Determine Asset Criticality

Having identified the system's assets and its related security goals, the project team embarked on the next step of determining asset criticality on the identified assets in the previous step. The criticality level is determined and assessed in greater detail as part of the asset identification and criticality activity. An assessor team consisting of the security analyst and other experts prioritises assets in terms of the security goals by applying a novel asset criticality system using fuzzy logic proposed in i-CSRMT process so that the most critical assets can be connected with top priorities. This step is conducted as a separate brainstorming exercise, and the primary goal is to determine the criticality of the assets formally approved by all project team members. The FACS allows experts to express their differences in the inference process with less bias and higher reliability. Therefore, asset criticality is determined using the method proposed in the process and each asset is assigned a level of criticality using fuzzy inputs and the crisp rating values in Table 4.4. The result is shown in Table 5.16 using i-CSRMT; however, we could not integrate fuzzy logic into the tool. Therefore, we used MATLAB to get the final asset criticality output. The list of assets may not be exhaustive, but it will include the assets most valuable to the organisation and its users.

Figure 5.22 shows the AC level for each asset (according to Very High Critical, High Critical, Medium Critical, Low Critical and Very Low Critical) which is mainly obtained using minimum-maximum inference, which considers the minimum of the antecedents of the maximum for aggregation and Defuzzification. Hence, each asset's AC falls under one of the five categories from low critical to very high critical as defined in Table 5.4. For example, SCADA system is given the input values (C=1), (I=2), (A=1), (ACC=3), (CON=4) by an assessor, the output value is (AC = "2.5") using the FACS. Traditionally, different sets of fuzzy input (C, A, I, ACC, CON) may generate an identical value of the fuzzy output (AC); however the assets may not necessarily be the same. Figure 5.23 displays a graphical chart of the total number of each asset criticality level, it changes over time.



**Figure 5.22: Asset criticality Result**



**Figure 5.23:** Asset criticality graphical chart

**Table 5.16: Asset criticality results**

Asset Name	Asset Description	Asset Goals					Fuzzy output	Asset Criticality Level
		Fuzzy input						
		C	A	I	CON	ACC		
Routers, firewalls, intrusion detection systems	Monitor, analyse and filter any harmful signs, while being connected to the corporate network.	1	3	4	4	1	2.5	Medium Critical
Databases	Stores sensitive information about its customers, personnel, marketing, landlords, tenants, transactions, assets, finances, and other information about the company's business process.	4	4	3	4	5	4	Highly Critical
Company and customer data	Represent sensitive and private information about employees, finances, assets.	3	3	3	4	4	3.5	Medium Critical
Web & Application Servers	Provides processes and delivers web contents such as images and assets information to employees and customers. The application server provides the platform for hosting frontend applications used by the company	1	3	3	1	1	2	Low Critical
SCADA Systems	Provides the user interface that allows employees and customers to visualise, access, and patronise the company's services.	2	5	5	1	4	3	Medium Critical

### **5.12.3. Activity 3: Threat Modelling**

Investigating how cybersecurity can be addressed for each critical asset is crucial. Therefore, this activity's goal is to identify as many potential threats and vulnerabilities as possible. The activity is organised as a workshop, drawn from actors with expertise in risk management. The actors involved in this activity include the security analyst and a member of senior management. Also, various methodologies and standards were employed at different steps of performing the threat modelling activity. All participating actors were briefed about the parts of the standard/methodologies used and its benefit.

#### **5.12.3.1. Step 1: Determine the Vulnerability profile**

The first step to secure these assets is to identify their vulnerabilities and weaknesses by examining the attack surface and the relevant threat models. The analysis team moved on to create a vulnerability profile that contains the vulnerabilities that are exploited and affect assets. To direct this process, the project's team members, a security analyst and system administrator were brought together to conduct an informed brainstorming session to identify a detailed list of potential vulnerabilities.

Secondly, a list of vulnerabilities compiled by CWE and CAPEC was presented to the team to understand by providing a standardised list of software weaknesses and the methods to exploit those weaknesses such that two or more people know they are talking about the same thing. Without standardisation, individuals are forced to engage in non-standard descriptive terms that generate rework and misunderstanding. In this regard, the team considered all potential vulnerabilities. Adopting these standards proved to be a simple yet effective way to identify, categorise and determine the likelihood of potential vulnerabilities, and it led to the participants having a better understanding of asset vulnerabilities. It also mitigates any problem that may arise due to using simplistic vulnerability categorisation and rating system, which are likely to be rejected by the team members. Thus, to document the assets' vulnerabilities, a template that shows several vulnerability factors is used. By identifying the weak points, the security analyst documents the meeting's result by filling a vulnerability profile for the study context, which affected critical assets and caused a threat that led to risk.

#### **5.12.3.2. Step 2: Determine Threat profile**

Having completed the asset inventory and identified vulnerabilities, the analysis team created a threat profile that identifies the threats that can potentially affect the assets and compromise sensitive information. To direct this process, the project's team members, a security analyst and system administrator were brought together to conduct an informed brainstorming session to identify a detailed list of threats, threat actor factors, TTP and IOC. A list of security threats compiled by CAPEC and WASC was presented to the team. Firstly, the team started with identifying a combined list of 10 security

threats that they perceived to be important to the organisation's assets. After a brief reconsideration, the list was updated with three additional threats.

Secondly, the adoption of these two threat classification models proved helpful and straightforward in identifying, categorising and determining the impact of potential threats, and it led to the participants having a better understanding of threat elements. With the adoption of CTI, a better understanding of threat actors, attack patterns, and TTP use is understood by the team. In this regard, the team considered all potential threats to document the threats, vulnerabilities, IOC and TTP associated with the assets; a template that shows several threat attributes is used. Figure 5.24 displays the threat actor factors, indicators of compromise (IOC), TTP, related attack patterns, execution flow and possible vulnerabilities. The security analyst documents the result of the meeting by filling a threat profile.

The screenshot displays the CSRMT (Cyber Security Risk Management Tool) interface. The main content area is titled 'Project #1 - IT Infrastructure Project For DISCOS' and is currently in 'In Progress' status. The 'Threat Modeling' tab is active, showing a detailed threat profile for 'Command Line Execution through SQL Injection'.

**THREAT MODELLING**

**Threat Name**  
Command Line Execution through SQL Injection

**Description**  
An attacker uses standard SQL injection methods to inject data into the command line for execution. This could be done directly through misuse of directives such as MSSQL\_xp\_cmdshell or indirectly through injection of data into the database that would be interpreted as shell commands. Sometime later, an unscrupulous backend application (or could be part of the functionality of the same application) fetches the injected data stored in the database and uses this data as command line arguments without performing proper validation. The malicious data escapes that data plane by spawning new commands to be executed on the host.

**Resources Required**  
None: No specialized resources are required to execute this type of attack.

**Skills Required**  
SKILL: The attacker most likely has to be familiar with the internal functionality of the system to launch this attack. Without that knowledge, there are not many feedback mechanisms to give an attacker the indication of how to perform command injection or whether the attack is succeeding.: LEVEL: High

**Related Attack Patterns**  
NATURE:ChildOf:CAPEC ID:66

**Indicators**

**Execusion Flow**  
STEP: 1: PHASE: Explore: DESCRIPTION: [Probe for SQL Injection vulnerability] The attacker injects SQL syntax into user-controllable data inputs to search unfiltered execution of the SQL syntax in a query. STEP: 2: PHASE: Exploit: DESCRIPTION: [Achieve arbitrary command execution through SQL Injection with the MSSQL\_xp\_cmdshell directive] The attacker leverages a SQL Injection attack to inject shell code to be executed by leveraging the xp\_cmdshell directive. STEP: 3: PHASE: Exploit: DESCRIPTION: [Inject malicious data in the database] Leverage SQL injection to inject data in the database that could later be used to achieve command injection if ever used as a command line argument. STEP: 4: PHASE: Exploit: DESCRIPTION: [Trigger command line execution with injected arguments] The attacker causes execution of command line functionality which leverages previously injected database content as arguments.

**Possible Assets Vulnerabilities**

- Improper Input Validation
- Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')

**ACTIVITY TIMELINE**

- New task added to the project. 10 months ago
- IT Infrastructure Project For DISCOS project details updated. 11 months ago
- IT Infrastructure Project For DISCOS project details updated. 11 months ago
- IT Infrastructure Project For DISCOS project details updated. 11 months ago
- IT Infrastructure Project For DISCOS project details updated. 11 months ago
- New file uploaded to the project.

Figure 5.24: Threat and vulnerability profile

#### **5.12.4. Activity 4: Risk Assessment**

The next activity involves a risk management process whose goal is to identify as many potential threats, vulnerabilities and risks as possible. The activity is organised as a workshop drawn from stakeholders with expertise in risk management. The stakeholders involved in this activity include the security analyst, information security officer, and senior management member. Also, various methodologies, machine learning techniques and standards were employed at different steps of performing risk management. All participating actors were briefed about the parts of the standard/methodologies used and its benefit.

##### **5.12.4.1. Step 1: Predict Risk Types**

In this step, a workshop is organised, which entails the identification of risks types. The participants are presented with multiple risk types, usually associated with critical infrastructure and assets of all kinds. The risk sources are provided by industry bodies and are updated regularly, which means that they provide up-to-date information about the most pressing security issues in information systems and web applications. In particular, a list of risks provided by the VCDB dataset is presented in the workshop, and the participants are challenged to select those they perceive to be relevant threats previously identified. We have used ten output categories of risks, and the value range for the features is from (R1 = Crimeware, R2 = Cyber espionage, R3 = Denial of service, R4 = Everything else, R5 = lost and stolen assets, R6 = miscellaneous errors, R7 = payment card skimmers, R8 = point of sale, R9 = privilege misuse and R10 = web applications) with possible classes. This is a multi-class problem, and we have the following risk types as output features. A list of risks is therefore identified.

##### **Phase 1: Prediction Result**

Table 5.17 presents the six classifiers' accuracy performance details in predicting the different risk types based on the given CSRM features (Assets, Controls, Threat Actor and TTP). Based on the Asset features, LR, DT and NB-Multi achieved 95%, 93% and 92% respectively for predicting risk type "Lost and Stolen Assets", "Everything Else", "Crimeware", "Cyber Espionage" and "Denial of Service". They failed to identify risk types "Point of Sale" and "Web Application". RF, KNN and NB achieved 87%, 86% and 71% respectively for predicting risk type "Crimeware", "Cyber Espionage", and "Lost and Stolen Assets". NN failed to predict any risk type and achieved 4%. Based on the TTP features, KNN, LR, NB-Multi, and DT achieved an accuracy of 80% for predicting risk type "Denial of Service", "Cyber Espionage" and "Everything Else". RF achieved an accuracy of 72% for predicting risk type "cyber espionage" and "Everything Else" NN failed to predict any risk type and achieved 4%.

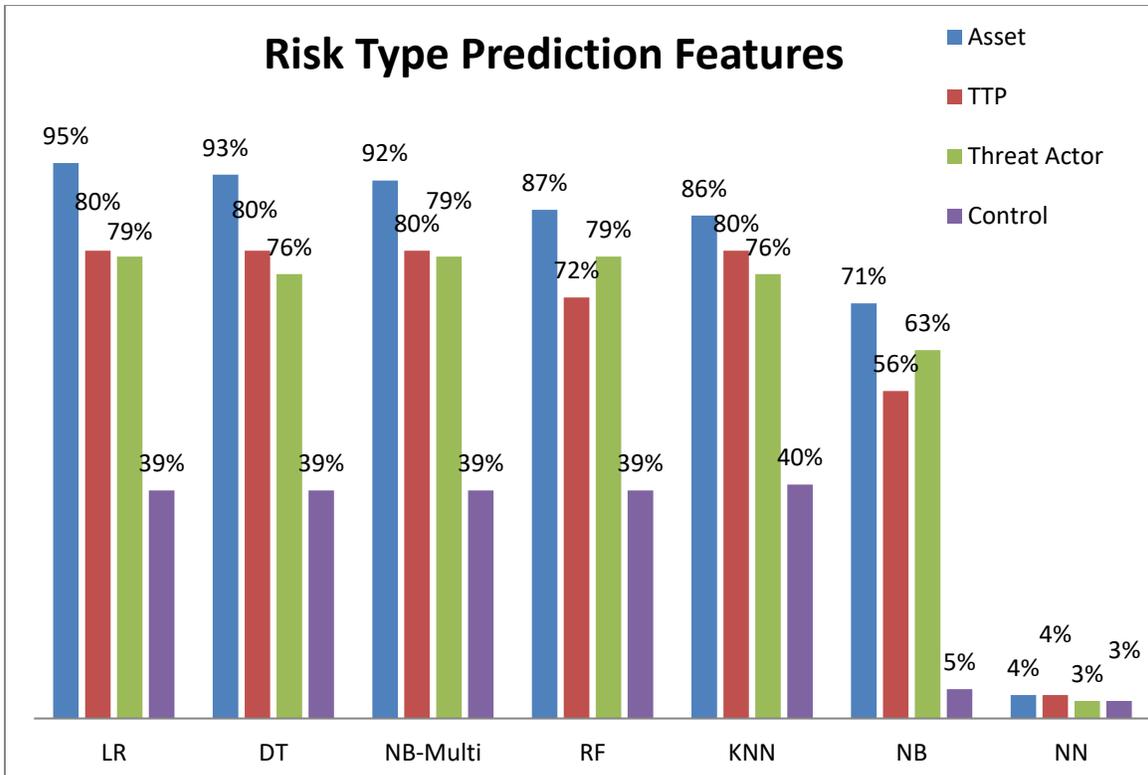
Based on the Threat Actor features, LR, NB-Multi and RF achieved 79% accuracy for predicting risk type "Everything Else", "Cyber Espionage" "Privilege Misuse", and "Crimeware". KNN could predict risk

type “Everything Else”, “Cyber Espionage”, and “Privilege Misuse” while DT could predict risk type “Everything Else”, “Cyber Espionage”, and “Crimeware” both classifiers with 76% accuracy. The NB achieved 63% accuracy for predicting risk types “” Cyber Espionage” and “Privileged Misuse”. NN achieved 3% accuracy and failed to predict any risk type. Lastly, based on the control features, KNN achieved the highest accuracy of 40% in predicting risk type “Everything Else”. LR, DT, NB-Multi and RF achieved 39% for predicting risk type “Everything Else”. NB and NN achieved an accuracy of 5% and 3% respectively. Both classifiers failed to predict any risk type. Asset and TTP features performed well on all the different classifiers except NN. Comparing the performance of all the features shows that NB failed to perform risk type prediction based on control features and NN achieved very low risk type prediction based on all the features. Therefore, for the risk types “Everything Else”, “Privilege Misuse”, “Denial of Service” and “Cyber Espionage” all the input features achieved high prediction. Table 5.17 shows that Asset and TTP are the best features to predict risk types presented in this work.

**Table 5.17:** Performance of the features on each of the classifiers for predicting risk types

Accuracy	Risk Type Prediction Features				
	Asset	TTP	Threat Actor	Control	Full
LR	95%	80%	79%	39%	39%
DT	93%	80%	76%	39%	39%
NB-Multi	92%	80%	79%	39%	39%
RF	87%	72%	79%	39%	39%
KNN	86%	80%	76%	40%	30%
NB	71%	56%	63%	5%	5%
NN	4%	4%	3%	3%	3%

Figure 5.25 displays the graphical chart representation of the Table 5.18 shows the percentage performance of each feature on each classifier.



**Figure 5.25:** Performance of the features on each of the classifiers for predicting risk types

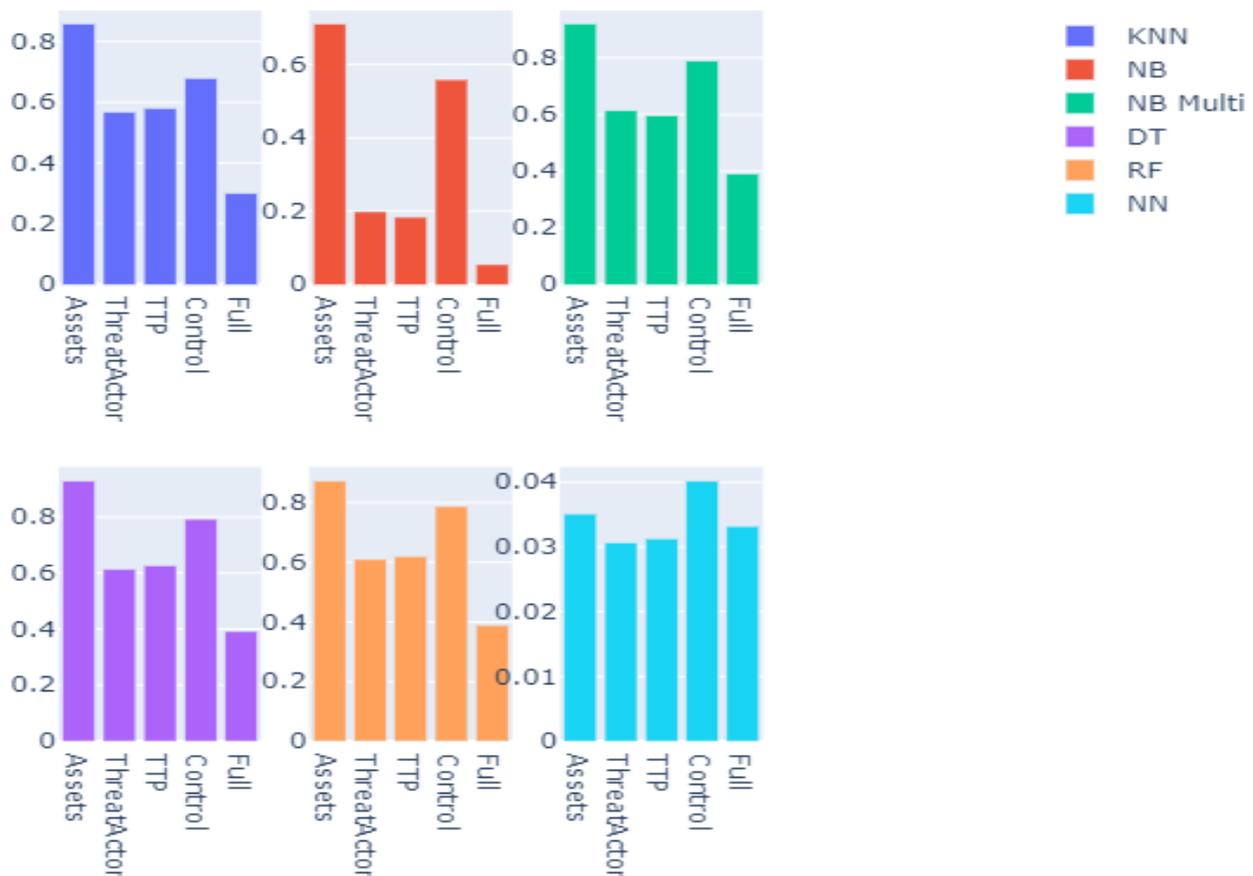
This is because different classifiers are based on different fundamentals. LR takes into account the probabilities of several independent variables describing the possible outcomes of a single trial using logistic functions. NB classifier takes into account posterior probability which might be good, DT takes into account the relationship between data into account and NN takes hidden relationships and find final relationship. In our case, DT performed because it is good in solving regression and classification problems, thereof it's performed better in predicting the risk types.

### Phase 2: Prediction Accuracy

After predicting the possible risk types by feeding the i-CSRMs features from VCDB dataset into our classifiers, the next step is to interpret the different classifiers' accuracy for various types of input features. Therefore, the predictive accuracy percentage of six different machine learning classifiers based on CSRMs features is presented. However, each feature performed differently within classifiers. The best overall predictive accuracy including all input features is recorded with Decision Tree (DT) algorithm which is (92.92%) on Asset features, Controls (79.26%), TTP (62.73%), Threat Actor (61.32%), and Full features was (39.12%). The second best algorithm is NB Multi which gave us (91.90%) on asset features, control features (78.88%), threat actor (61.33%), TTP (59.54%) and full features gave us (39.05%). The

third best algorithm is RF, it performed well on Asset features with (87.36%), control (78.75%), TTP (62.03%), Threat Actor (61.01%) and full features (38.93%). The fourth best algorithm is KNN, it performed well on almost all the input features, Asset features (85.77%), Controls (67.96%), TTP (58.07%), Threat Actor (56.80%) and the full features produced the least accuracy with (29.99%). The fifth best algorithm is the NB algorithm that performed well on the asset features with (71.03%), controls (55.90%), Threat Actor (19.85%), TTP (18.38%) and full features with (05.42%). The sixth algorithm which is NN didn't perform well on all the features, control features is (04.02%), Asset features is (03.51%), Full feature is (03.32%), TTP (03.13%) and threat actor (03.06%).

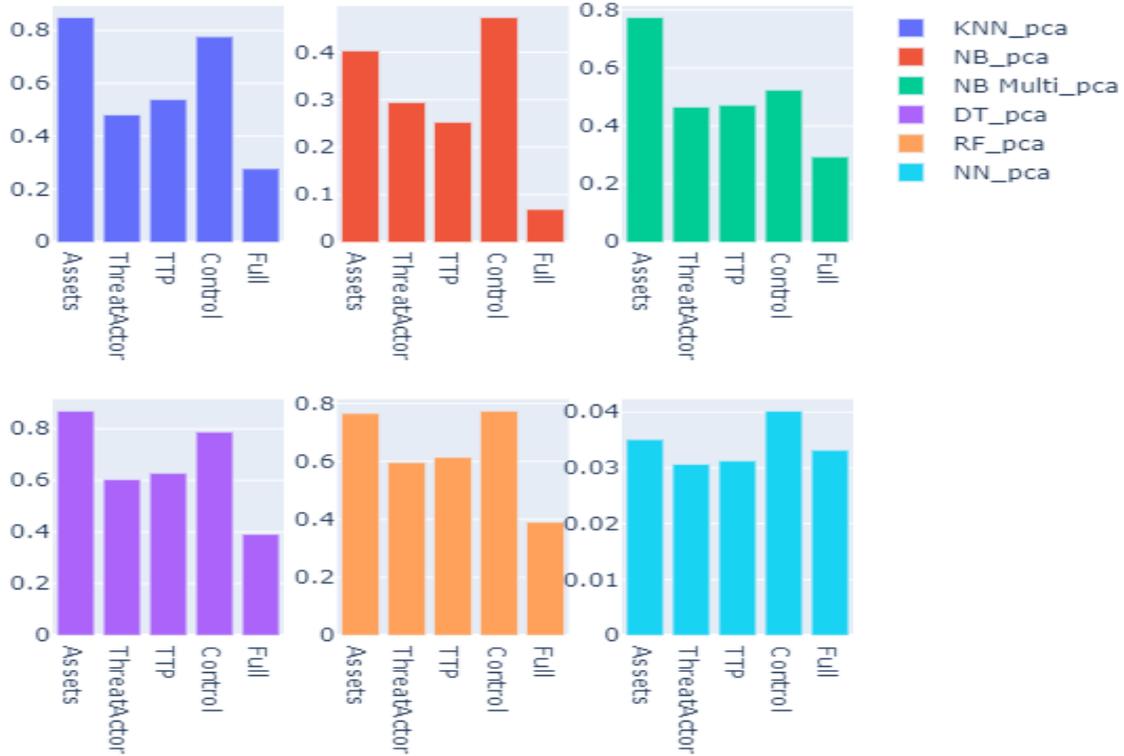
This shows that the Asset features performed well with DT (92.92%), NB Multi (91.90%), RF (87.36%), KNN (85.77%) and NB (71.03%). NN did not perform well with (03.51%). The control features also performed well with DT (79.25%), NB Multi (78.88%), RF (78.74%) and KNN (67.96%). On the other hand, Neural Networks (NN) and Naïve Bayes (NB) did not make satisfactory prediction accuracy on all the features. It can be noted that the most prominent features to detect risk types are Assets and control features. The result clearly shows that DT outperformed other classifiers giving the highest satisfactory accuracy for the VCDB dataset for risk type prediction.



**Figure 5.26:** The accuracy of different classifiers for various types of input binary features

**Phase 3: Results of the different classifiers transformed by PCA**

Figure 5.27 shows the results of different classifiers for various kinds of input features that have been transformed by applying PCA. We figure out that, PCA does improve accuracy for TTP and Control features where the accuracy is above 79%.



**Figure 5.27:** The accuracy of different classifiers for various types of features transformed by applying PCA

**Phase 4: Results of Confusion Matrix:** This section describes the classifiers’ performance on the test data for which the true values are known. This allows for the visualization of the performance of an algorithm. In this case, the best overall predictive accuracy was recorded with DT which produced better results than other classifiers as shown in Appendix C.

**Phase 5: Analyzing the results of the DT algorithm for identifying the different types of risk:** Figure 5.28 shows the DT classifier with a precision of 100% in identifying Crimeware (R1), 70% precision was obtained for cyber espionage (R2), 73% precision for Denial of Service (R3), 77% precision for

Everything else (R4) and 74% precision for lost and stolen assets (R5). The precision of 61% for Miscellaneous Error (R6), Precision of 82% for payment card skimmer (R7), Precision of 82% for point of sale (R8), Precision of 95% for privilege misuse (R9) and a precision of 26% for web application (R10).

The DT classifier shows a recall of 53% in identifying Crimeware (R1), 69% recall was obtained for cyber espionage (R2), 50% recall for Denial of Service (R3), 58% recall for Everything else (R4) and 56% recall for lost and stolen assets (R5). Recall of 34% for Miscellaneous Error (R6), Recall of 43% for payment card skimmer (R7), Recall of 37% for point of sale (R8), Recall of 71% for privilege misuse (R9) and a recall of 71% for web application (R10).

The DT classifier shows an F1-score of 69% in identifying Crimeware (R1), 69% F1-score was obtained for cyber espionage (R2), 69% F1-score for Denial of Service (R3), 66% F1-score for Everything else (R4) and 64% F1-score for lost and stolen assets (R5). F1-score of 44% for Miscellaneous Error (R6), F1-score of 57% for payment card skimmer (R7), F1-score of 51% for point of sale (R8), F1-score of 81% for privilege misuse (R9) and an F1-score of 39% for web application (R10).

Therefore, DT achieved a very high precision of 100% in identifying Crimeware (R1) and a Precision of 95% in identifying privilege misuse (R8). DT achieved a high Recall of 71% in identifying privilege misuse (R9) and web application (R10). Finally, an f1-score of 81% for identifying privilege misuse (R9) is achieved.

#### **5.12.4.2. Step 2: Determine Risk Level**

After identifying the various IOC, TTP, vulnerabilities, threats, and predicted the risk types using dataset, we identified and assessed the risks by estimating the assets' likelihood and impact. The Web pages allow the organisation to adapt various aspects associated with risks and their relations. This includes risk types, risk impact, risk likelihood and control measures.

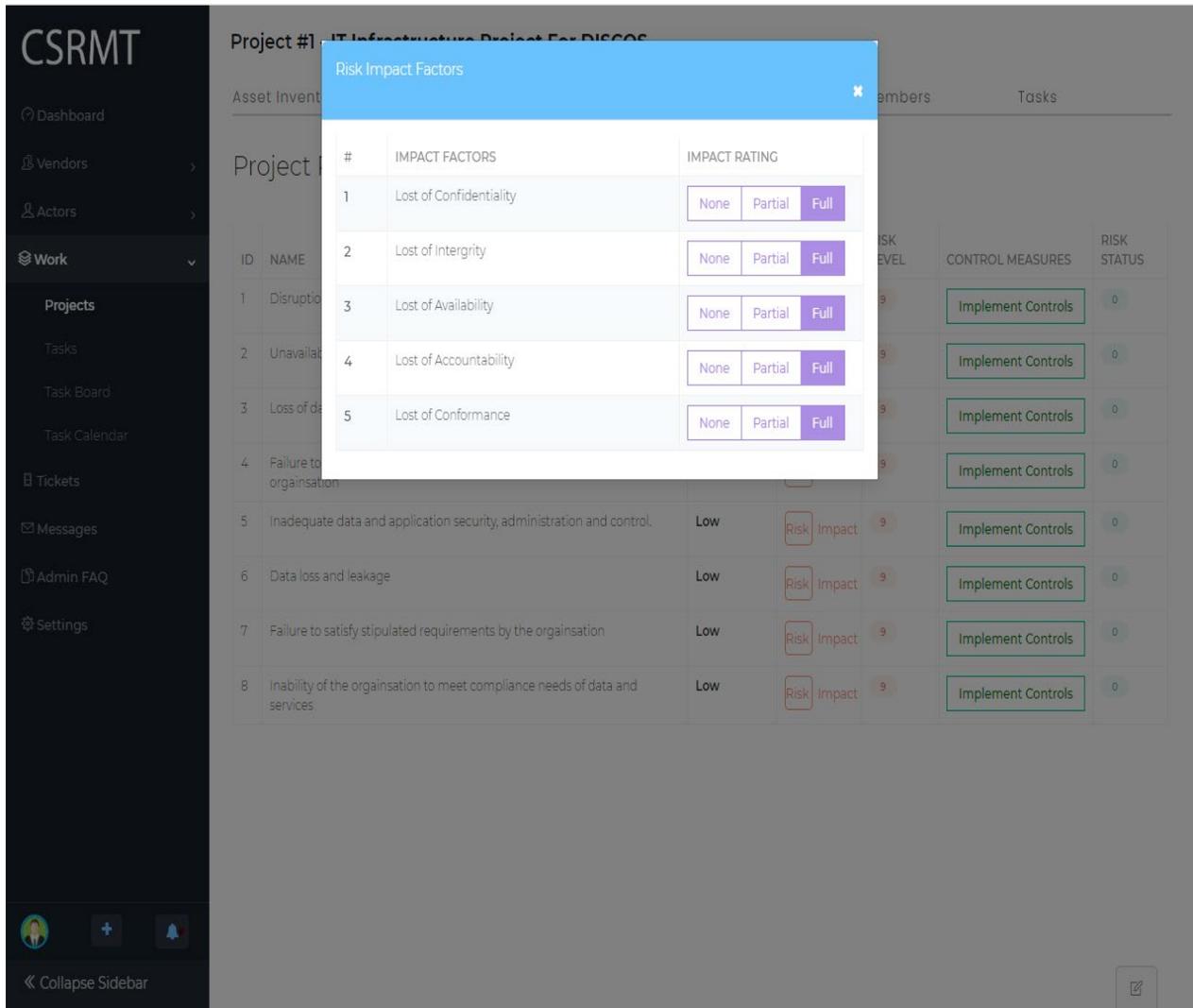
- **Phase 1- Estimating Risk Likelihood:** To estimate the overall likelihood of the risk, threat actor and vulnerability factors are put into consideration. The overall likelihood falls within high, medium and low, sufficient for the overall risk score shown in Figure 5.14.

The screenshot shows the CSRMT web application interface. On the left is a dark sidebar with navigation options: Dashboard, Vendors, Actors, Work (expanded), Projects, Tasks, Task Board, Task Calendar, Tickets, Messages, Admin FAQ, and Settings. At the bottom of the sidebar are user profile icons, a plus sign, a notification bell, and a 'Collapse Sidebar' button. The main content area is titled 'Project #1 - IT Infrastructure Project For DISCOS' and has tabs for 'Asset Inventory', 'Threat Modeling', 'Risk Assessment' (selected), and 'Controls Eff'. Below the tabs is the heading 'Project Risk Assessment' and a table with the following data:

ID	NAME	LIKELIHOOD
1	Disruption of business process	High
2	Unavailability of critical data and assets	High
3	Loss of data integrity and unauthorised changes to assets	High
4	Failure to provide security transparency and accountability by the organisation	High
5	Data loss and leakage	High
6	Inability of the organisation to meet compliance needs of data and services	High

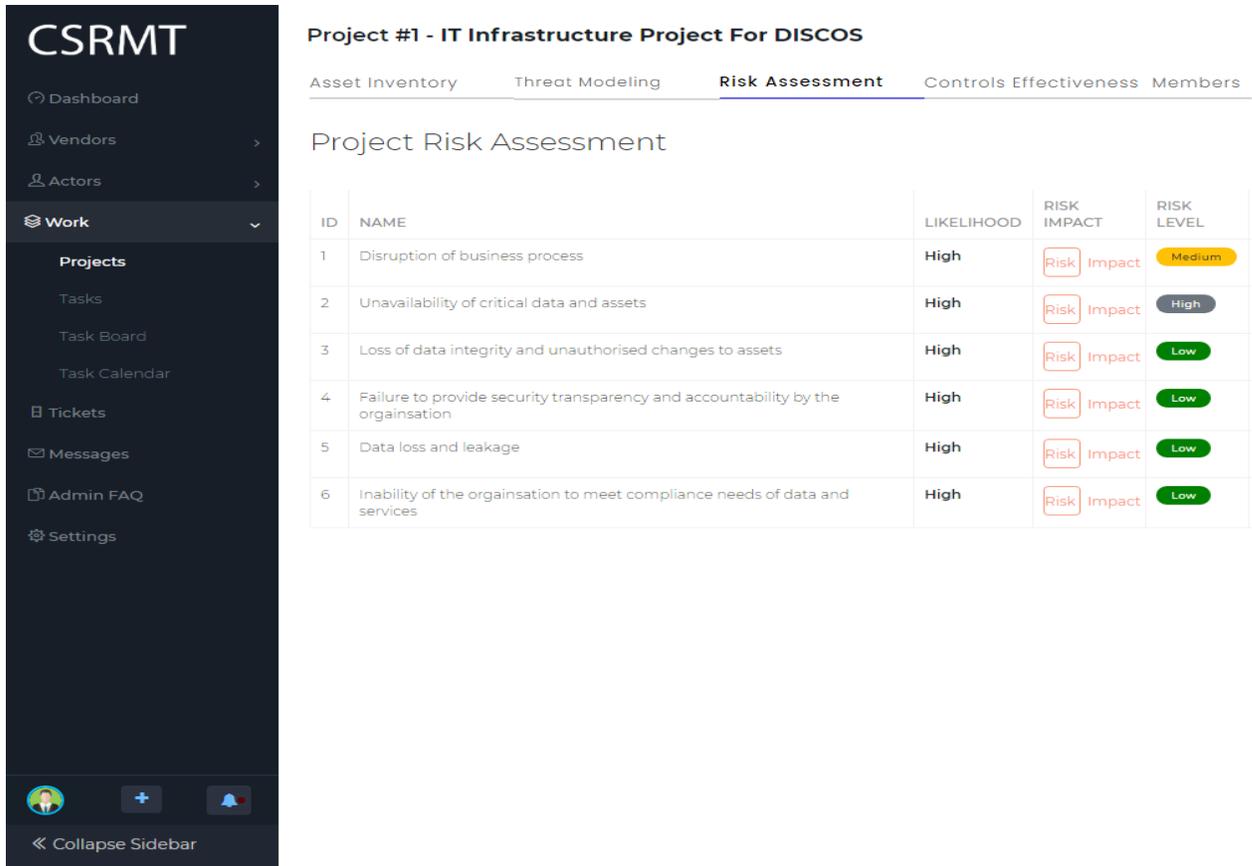
**Figure 5.14:** Risk likelihood

- **Phase 2- Estimating Risk Impact:** The web page allows the organisation to associate the defined risk types with the asset goals. This is done by selecting None, Partial or Full as shown in Figure 5.15.



**Figure 5.15:** Risk Impact factor selection

- Phase 3- Determine Risk Level:** The web page displays the results of the risk calculation. Each risk event is evaluated and presented separately with the elements used in the calculation and the calculated risk value. Figure 5.16 presents the calculated risk value which represents how dangerous the risk is to the organisation.



**Figure 5.16:** Calculated Risk Level

### 5.12.5. Activity 5: Risk Controls

The next activity involves identifying risk controls, organised as a workshop involving the risk management team members who decide and establish security controls from different perspectives that any potential critical infrastructure must meet. During the seminar, the security analyst presented the risk register while also repeating the need to evaluate the effectiveness of existing risk control and develop a new compilation of security controls from CIS\_CSC. We first identified existing controls to ensure that the controls worked correctly and evaluated the existing controls' effectiveness in step 2. If controls do not work correctly, we have detected the controls that need to be implemented to address the identified risks.

### 5.12.5.1. Step 1: Identification of Existing Control Types

We first identified DisCos existing controls to ensure that the controls are working correctly. The organisation detected the controls; some are shown in Table 5.19 to address the identified risks. The outcome determines the security control budget for the organisation, and decisions are optimised.

**Table 5.19:** Existing Control Types

Control type	Attack Techniques	Control description
Preventive	Brute Force	After a certain number of a failed login attempt to prevent passwords from being guessed, set account lockout policies.
	Disabling security tools	The proper process, registry, and file permission should be in place to prevent the anonymous organisation from disabling or interfering with the Disco's security services.
Detective	Account discovery	Identify unnecessary system utilities or potentially malicious software that may be used to acquire information or data about system and domain accounts, and block them by using whitelisting tool or software restriction policies where appropriate.
	System Network Configuration Discovery	
	File and Directory Discovery	
	Data from the local system	
	Spear-phishing attachment	Network intrusion prevention systems should be put in place to scan and remove malicious e-mail attachments.
Corrective	External Remote Services	Limit access to remote services through centrally managed VPNs, and other managed remote access internal systems through network proxies, gateways and firewalls.
		Use strong two-factor or multi-factor authentication for remote service accounts to mitigate the anonymousorganisation's ability to leverage stolen credentials.
	Credential Dumping	Ensure that administrator accounts have complex, unique passwords across all systems on the network.
	E-mail Collection	Use of two-factor authentication for public-facing webmail servers is recommended as a best practice to minimise the use of usernames and passwords to the anonymousorganisation.
	Forced Authentication	Use strong passwords to increase the difficulty of credential hashes from being cracked if they are obtained.
	User Execution	Training is required for the Disco employees to raise awareness on raising suspicion for potentially malicious events.
	Spear-phishing attachment	Antivirus can also be used as it automatically isolates suspicious files

### 5.12.5.2. Step 2: Evaluating the Effectiveness of Existing Controls

It was proposed that control effectiveness should be specified according to five fundamental categories namely: relevance of the control, strength of the control, coverage of the control, integration of the control and traceability of the control. The participants became involved and based on their expert opinion; effectiveness of the existing controls is specified in Figure 5.17.

ID	RISK NAME	IMPLEMENTED CONTROL	RATING FOR RELEVANCE	RATING FOR STRENGTH	RATING FOR COVERAGE	RATING FOR INTEGRATION	RATING FOR TRACEABILITY	OVERALL CONTROL EFFECTIVENESS
17	Disruption of business process	Remove Users From Local Administrator Group On Systems	CRITICAL (5)	MINOR (2)	MODERATE (3)	MAJOR (4)	MINOR (2)	16 (MAJOR)
16	Inability of the organisation to meet compliance needs of data and services	Microsoft Enhanced Mitigation Experienced Toolkit (EMET) Attack Surface Reduction (ASR) Feature Can Be Used To Block Methods Using Rundll32.exe To Bypass Whitelisting	MINOR (2)	MODERATE (3)	MINOR (2)	MODERATE (3)	MODERATE (3)	13 (MODERATE)
15	Disruption of business process	System Hardening E.g. Patch Management And Systems	MODERATE (3)	CRITICAL (5)	MAJOR (4)	CRITICAL (5)	CRITICAL (5)	22 (CRITICAL)

Figure 5.17: Control Effectiveness Result

### 5.12.5.3. Step 3: Implement Control Measures to Determine New Risk Status

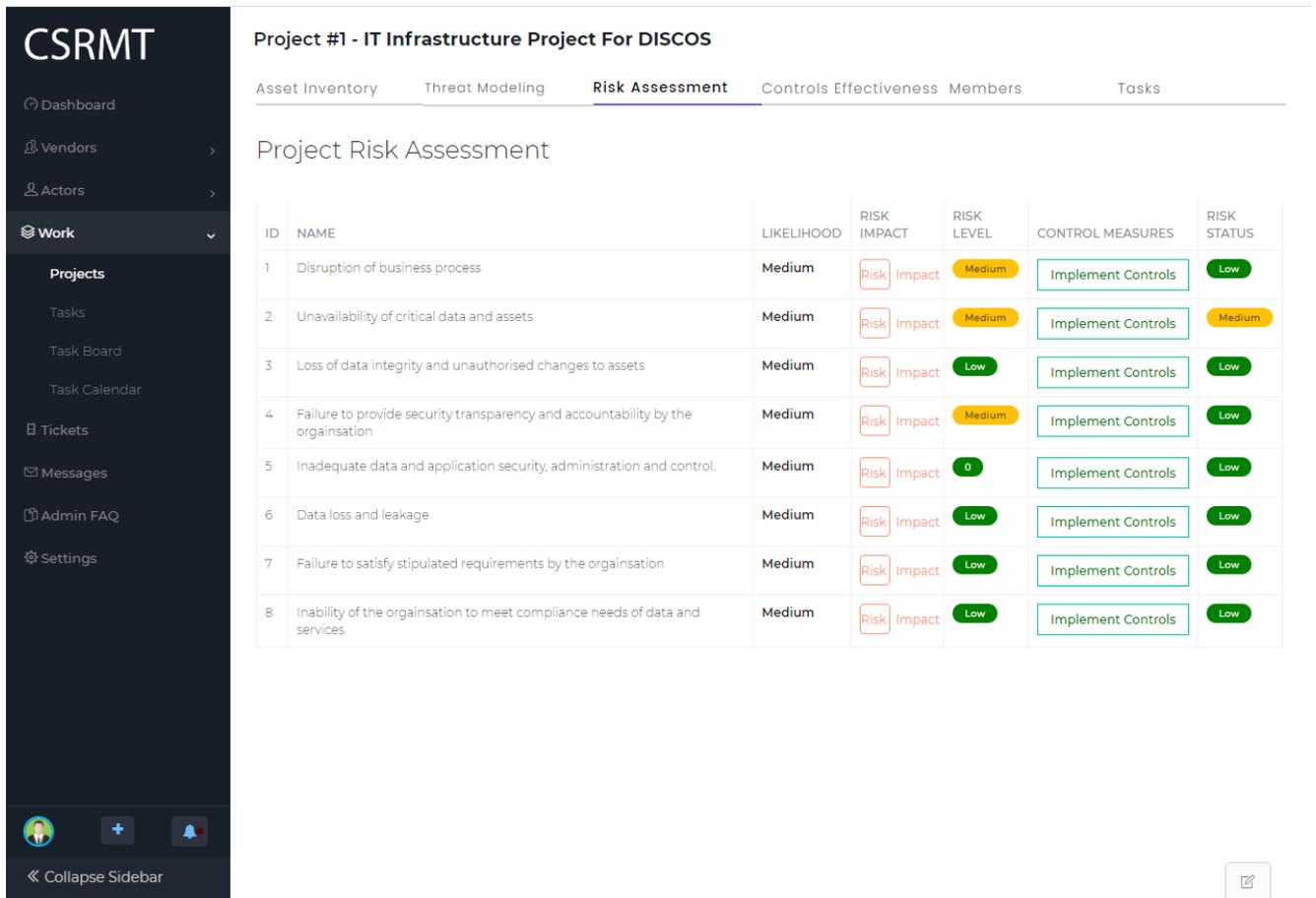
We first identified existing controls, to ensure that the controls are working correctly. The Web page allows the organisation to define a list of available controls. The user can select the control measure using the control rating: None, partial and full as shown in Figure 7.18 to address the identified risks.

The screenshot displays the CSRMT application interface. A modal window titled "Risk Control Measures" is open, showing a table of 14 control measures. The table has columns for "#", "CONTROL NAME", and "CONTROL RATING". The ratings are "None", "Partial", or "Full". The background shows a sidebar with navigation options and a main content area with a table of risk items.

#	CONTROL NAME	CONTROL RATING
1	Compliance Program	None Partial Full
2	Data leakage prevention	None Partial Full
3	Adequate staff training	None Partial Full
4	Data Loss Prevention Mechanism	None Partial Full
5	Security Incident Report	None Partial Full
6	Accuarate Usage Estimation	None Partial Full
7	Need to isolate some network systems	None Partial Full
8	Microsoft Enhanced Mitigation Experienced Toolkit (EMET) Attack Surface Reduction (ASR) feature can be used to block methods using rundll32.exe to bypass whitelisting	None Partial Full
9	Remove users from local administrator group on systems	None Partial Full
10	System hardening e.g. patch management and systems monitoring activities, anti-virus and intrusion prevention system.	None Partial Full
11	Apply access control measures	None Partial Full
12	Recommend network segmentation	None Partial Full
13	Special access points into the network should be documented, controlled, monitored and limited	None Partial Full
14	Connections between networks should be heavily regulated through the use of a demilitarized zone	None Partial Full

**Figure 7.18: Control measure implementation**

Figure 7.19 displays the current risk status for each risk type. It presents the risk type and their calculated risk values and the control measures that can be used to mitigate the risk.



**Figure 7.19: Risk Assessment overview**

#### 5.12.5.4. Risk Register

Based on reviews from other members, the research team established a threat profile; the threat classification and impact ranking have now been approved. The language required for starting to define and evaluate risks that can affect assets has been established. The research team started a series of organised workshops to define threats, estimate likelihood and impact, and implement control measures.

The first workshop included risk identification. Many sources of threats were posed to participants, typically correlated with all forms of assets. The industries have provided the sources of risk and are regularly updated to include up-to-date details on critical assets' highest security threats. Specifically, the workshop included a set of risks offered by CAPEC and the participants had to choose the risks they consider important. There was a cumulative list of 23 threats, although it was shortened to 15 later.

To quantify the likelihood and impact values of the identified threats, the second Workshop was conducted. During the workshop, all participants were asked to provide the best possible estimation.

Therefore, the methodology for risk rating OWASP was presented. As the participants represent different skills, they presumably have different opinions about the risk probability assessment and the impact values, which is the key concept behind the OWASP approach.

Finally, another workshop was held to identify the control measures needed to reduce or apprehend risk. The analysis team was presented with a collection of alternative controls by CSC CIS during this exercise. These controls provide a robust list of best practises to alleviate most types of risk. The research team then discussed possible control measures and concluded which measures would control or minimise risk to acceptable level. The CSC CIS took most control steps, while others were obtained from ENISA, especially when CSC CIS did not monitor those risks. Finally, a risk register showing the threats, likelihood, impacts and control measures was developed.

**5.13. Feedback Review Findings for i-CSRMT Framework**

This section analyses the feedback from stakeholders after implementing the i-CSRMT Framework. The review’s focus would be to evaluate the reliability of i-CSRMT in support of critical infrastructure for risk management from the perspective of stakeholders. Table 5.20 shows the total number of responses collected.

**Table 5.20:** Feedbacks from Case-Study participants and Respondents

Case Study	Participants		Respondents	
	Senior Management	IT Staff	Senior Management	IT Staff
Case Study	15	35	12	28
Total	<b>50</b>		<b>40</b>	

Appendix A shows the relevance and acceptability outcomes for the i-CSRMT Framework and i-CSRMT based on the assessment parameters (ease of use, relevance, usefulness, flexibility and dynamics, conformity to security requirements and industry standards, trustworthiness). The compiled results of the stakeholders’ feedback based on the assessment parameters are presented below.

**5.13.1. Ease of Use Parameter**

According to the results of the analysis, 10 out of 40 stakeholder respondents (25%) completely agreed that the proposed i-CSRMT Framework is simple to use, 19 respondents (47.5%) agreed that the Framework is simple to follow. 7 respondents (17.5%) are undecided on whether or not the system is simple to use, 4 respondents (10%) completely disagreed to the frameworks usability. As seen in Table

5.21, 72.5% of respondents believe the Framework is straightforward and convenient to use by the organisation.

**Table 7.21:** Stakeholders' Views on the i-CSR Framework's Ease of Use

<b>Ease of Use</b>		
<i>Do you agree the i-CSR Framework is simple and easy to understand for the intended audience?</i>		
<b>Response Selections</b>	<b>Number of Response</b>	<b>Total %</b>
Completely Agree	10	25 %
Agree	19	47.5%
Partially agree	7	17.5%
Completely Disagree	4	10%

### 5.13.2. Relevance Parameter

In terms of the Framework's relevance in supporting the organisation to achieve risk management, 37.5% of respondents firmly agreed, and 45% agreed that the Framework is important in assisting the organisation in achieving overall risk management. Furthermore, 12.5% of respondents were unsure of its significance. These results show that the suggested structure is appropriate for dealing with risk management challenges at the organisational level. Table 5.22 illustrates this.

**Table 5.22:** Framework's relevance for supporting the organisations achieve risk management

<b>Relevance</b>		
<i>Do you think the proposed Framework is applicable for assisting organisations with risk management?</i>		
<b>Response Selections</b>	<b>Number of Response</b>	<b>Total %</b>
Completely Agree	15	37.5%
Agree	18	45%
Partially agree	5	12.5%
Completely Disagree	2	5%

### 5.13.3. Usefulness Parameter

A positive change in stakeholders' ratings is observed based on the Framework's usefulness in delivering organisation needs. As seen in Table 5.23, 87.5% of the stakeholders concluded that the process is beneficial for achieving the intended outcomes.

**Table 7.23:** Responses on the Usefulness of i-CSR Framework

<b>Usefulness</b>		
<i>Do you think the proposed Framework will help you meet the desired goals and objectives?</i>		
<b>Response Selections</b>	<b>Number of Response</b>	<b>Total %</b>
Completely Agree	25	62.5%
Agree	10	25%
Partially agree	4	10%
Completely Disagree	1	2.5%

#### **5.13.4. Flexibility Parameter**

The proposed Framework was developed with the intent of adapting to complex and evolving situations in mind. According to Table 5.24, 47.5% of the stakeholder respondents completely agreed that the Framework is flexible and 35% agreed that it is quite flexible. As seen in Table 5.24, the overall % of those who agreed are 82.5%, which is higher than those who partially agreed (15%) and those who completely disagreed (2.5%) with the Framework’s versatility.

**Table 5.24:** Responses on the Flexibility of i-CSR Framework

<b>Flexibility</b>		
<i>Do you accept that the proposed Framework is adaptable to changing circumstances?</i>		
<b>Response Selections</b>	<b>Number of Response</b>	<b>Total %</b>
Completely Agree	19	47.5%
Agree	14	35%
Partially agree	6	15%
Completely Disagree	1	2.5%

#### **5.13.5. Conformity to Security Requirements and Industry Standards**

The development of the Framework was based on a range of security standards and common practises. As seen in Table 5.25, the Framework’s conformity with applicable laws and regulations received the maximum acceptability rating, with 85% of respondents believing that it complies with applicable laws and regulations.

**Table 5.25:** Compliance with procedural laws, standards, and best practises is given a score based on the Framework’s compliance.

<b>Conformity to Security Requirements and Industry Standards</b>		
<i>Is the Framework following all applicable rules, guidelines, and best practises?</i>		
<b>Response Selections</b>	<b>Number of Response</b>	<b>Total %</b>
Completely Agree	20	50%
Agree	14	35%
Partially agree	4	10%
Completely Disagree	2	5%

### 5.13.6. Trustworthiness Parameter

Trustworthiness is a general concept that relates to a framework’s ability to deliver results that satisfy its users’ standards. As per stakeholder reviews, the Framework’s trustworthiness ranking received the lowest rating in this category. According to the approval rating, 75% of respondents thought the i-CSR Framework was trustworthy, whereas 15% partially agreed. However, 10% of the respondents disagreed that the Framework is feasible. According to the ratings’ findings, the Framework’s trustworthiness ranking is validly important, as seen in Table 5.26.

**Table 5.26:** Responses to the i-CSR Framework’s Trustworthiness

<b>Trustworthiness</b>		
<i>Do you think the new Framework would protect your security and privacy?</i>		
<b>Response Options</b>	<b>Response (Count)</b>	<b>Response (Percentage)</b>
Completely Agree	12	30%
Agree	18	45%
Partially agree	6	15%
Completely Disagree	4	10%

### 5.14. Case Study Implementation Results and Lessons Learnt

Stakeholder feedback was analysed using assessment parameters drawn from the well-known TAM and UTAUT models. The study was used to assess if the proposed Framework met its expected goals of facilitating and improving risk management, as stated in the research objectives. The study yielded promising findings in terms of stakeholders’ general perceptions of the i-CSR Framework’s acceptability. This confirmation is based on the overall affirmative responses received when “Completely

Agree” and “Agree” are merged to assess respondents’ confidence on both of the assessment parameters, as highlighted below:

- Ease of use: 72.5% of respondents thought the i-CSRMT Framework was simple to use.
- Relevance: 82.5% of respondents thought the i-CSRMT Framework was important.
- Usefulness: 87.5 % of respondents thought the i-CSRMT Framework was beneficial.
- Flexibility: 82.5% of respondents thought the i-CSRMT Framework was versatile.
- Conformity to Security Requirements and Industry Standards: 85% of the respondents believed the i-CSRMT Framework to be compliant.
- Trustworthiness: 75% of respondents thought the i-CSRMT Framework was trustworthy.

Based on the total summation of the responses, it can be determined that an average of 81% of respondents approved the proposed i-CSRMT Framework, with just around 19% expressing contrary opinions. In a positive vein, respondents shared enthusiasm and respect for the i-CSRMT Framework for providing adequate coverage of their needs. They admitted that it has a positive effect on the organisations’ ambitions for managing cyber risks. This allows one to conclude that some of the research objectives have been met.

Also, the researcher made several important findings during the process evaluation, such as the significance of organisations adopting a simplified methodology that focuses on risk management to direct their achievement of strategic, organisational, and financial goals rather than a generalised approach. The i-CSRMT Framework activities are systematic, clear, and straightforward, with no necessary financial or personnel strain to the organisation. The majority of the process tasks are simple to execute; however, the machine learning step might necessitate thorough preparation and guidance. The stakeholders who participated in the exercise were able to complete the measures without any bottlenecks or significant difficulties. More specifically, the study discovered that an inability to correctly define standards focusing on risk management and sufficiently probe critical infrastructure internal practises is likely to result in significant problems that cannot be corrected.

### **5.15. Summary of the Chapter**

The empirical analysis of the i-CSRMT Framework and i-CSRMT was explored in this chapter. Using a case-study method, the chapter presented a systematic discussion of empirical findings for verifying this research. The questionnaire methodology allowed the collection of reviews from participants who evaluated the i-CSRMT Framework to determine the relevance and acceptability of the proposed Framework. Stakeholders’ feedback was gathered and used to assess their perceptions and views on the

Framework's relevance and acceptability. Stakeholders shared confidence and fair satisfaction. The findings demonstrated that the proposed Framework is extremely important for assisting organisations in achieving overall risk assessment and risk type prediction.

## CHAPTER SIX

### DISCUSSION

#### 6.1. Introduction

This chapter discusses the findings of the empirical research conducted in Chapter 7 through the case study analysis. The chapter explains how and why the research questions were addressed and justified. It further offers an overview of the study results and focuses on how the findings help the research aim and objectives. Furthermore, the chapter emphasizes the need for a critical infrastructure integrated cybersecurity risk management (i-CSR) framework.

#### 6.2. Comparison between i-CSR Framework with other Works

This section compares the results of this research with those of other research studies published in the literature, focusing on findings that enhance critical infrastructure cybersecurity risk management. The researcher will then generalise the results and classify the risk management background factors utilizing this approach.

To create a comparison, some of the most important research papers and industry projects that tend to discuss the problem of risk management in critical infrastructure were chosen to assess general correlation and contrast with i-CSR. The number of comparative parameters is often specified in the form of questions. The questions are focused on the thesis's specific contributions, including tool support, risk management conceptualization, industry standards and best practices implementation, and the approach's assessment process. The results of the comparison are detailed in the parts that follow.

#### 6.3. Criteria for Reference Comparison

The reference criteria are derived from questions posed about the thesis's main contributions. As a result, the contribution is illustrated, accompanied by a summary and the related query. Table 6.1 displays the contrast parameters.

The comparison parameters are generated by formulating questions concerning the critical contributions of this thesis. Therefore, the contribution is highlighted, followed by the associated question and a brief description. The comparison parameters are shown in Table 6.1.

**Table 6.1: Comparison Parameters**

Parameter	Question	Details
Tool Support	<i>Does the literature provide tool support towards cybersecurity risk management?</i>	Each approach is analysed based on automated tool support that augments and enhances risk management from a critical infrastructure point of view through computation, analysis, visualisation, and evaluation. An automated tool to support the risk management activities is to minimize the efforts required to perform the risk management activities and provide accurate information about the risks based on the threat and vulnerability information to implement the proper controls. Therefore the tool aims for an effective risk management practice within critical infrastructure. Such a tool potentially strengthens cybersecurity risk management by making risk assessments and expert judgment procedures more effectively and timely. Thus, it is essential to have strong tool support, thereby facilitating and improving risk management's effectiveness (McNeil, Frey and Embrechts, 2015).
The conceptualisation of cybersecurity risk management	<i>Does the literature establish and decompose the fundamental concepts necessary for i-CSR?</i>	It is paramount for each approach to dissect cybersecurity risk management from a critical infrastructure point of view by laying the foundational knowledge on critical concepts. (Van den Berg <i>et al.</i> , 2014) emphasised the need for an approach that identifies, analyse and represents risk management from the eyes of conceptual knowledge to enhance understanding and provide reference points to critical infrastructure.
Adoption of industry standards	<i>Does the literature leverage and integrate industry standards?</i>	Industry standards provide a significant assertion to organisations that critical best practices are followed and assurance that all operations are executed according to generally accepted security principles. This is due to the global acceptance of industry standards, best-practice, and frameworks (Lewis, 2006).
Integrating Machine learning techniques within risk management activities	<i>Does the literature leverage and integrate machine learning techniques within the risk management activities?</i>	Introducing the machine learning framework for automation of risk identification is vital to securing the critical infrastructure. The Framework takes data, builds the features, applies machine learning algorithms and gives results.
The comprehensive implementation process of the proposed Framework	<i>Has the literature defined a comprehensive implementation process for the proposed Framework?</i>	The implementation process is a vital feature of every proposed approach. A process should provide a step-by-step actionable guideline for implementing the proposed conceptual model, Framework to critical infrastructure to accomplish risk management.

## **6.4. Discussion on Comparison Findings**

This section displays the comparison results between i-CSRMT and i-CSRMT with other risk management approaches based on five critical parameters peculiar to this research's contributions. The following section elaborates the comparison findings.

### **6.4.1. Tool Support**

There is substantial similarity in tool support, either fully or partially, amongst risk management tools and those presented in the existing literature. For instance, (Creasey and Marvell, 2013) developed IRAM designed for business-led information risk analysis methodology. IRAM provides businesses with tools for impact assessment, threat and vulnerability assessment and selection of the control. Also, STREAM (Creasey and Marvell, 2013) provides an attractive, low-cost alternative to spread sheets for governance, risk and compliance (GRC), scalable from free single-user to Enterprise-wide deployment of the most prominent organisations. STREAM has the advantage in that its framework mappings allow controls to be mapped to asset classes and Threats. Each time an Asset is added to an asset class, STREAM will automatically map all relevant controls and threats to the asset. The CIRAS tool (Bialas, 2016a) supports the selection of security measures for critical infrastructure by considering the impact of typical CI occurrences like interdependencies, cascading, and escalating the incident. Hence, the most noticeable similarity between i-CSRMT and the results in that literature is that they all support a holistic assessment of all aspects of C.I.s security measures, which includes the expected risk. However, the difference between these works and i-CSRMT is that they mainly focus on risk assessment. The i-CSRMT supports the i-CSRMT process to minimize the efforts required to perform the risk management activities and provide accurate information about the risks based on the CTI concepts to calculate the risk level.

### **6.4.2. Conceptualization of Cybersecurity Risk Management**

Understanding the factors relating to cybersecurity risk management in critical infrastructure is fundamental because it simplifies and consolidates prior knowledge in the domain. The significant research efforts on risk management have produced many propositions, and they all have different views and interpretation of security transparency concepts (Alcaraz and Zeadally, 2015). The authors (Cardenas et al., 2009) discussed the challenges for securing critical infrastructure and analyzed security mechanisms for prevention, detection and recovery, resilience and deterrence of attacks for securing CPS. In (Sridhar, Hahn and Govindarasu, 2012b), a layered approach is proposed for evaluating risk based on security to prevent, mitigate and tolerate attacks both on real power applications and cyber infrastructures. In (Wu, Kang and Li, 2015), the authors proposed a quantitative risk assessment model that provides users with attack information such as the type of attack, frequency, and target and source host identity. Authors

(Livadas et al., 2006) proposed a new approach for critical infrastructure asset identification using multi-criteria decision theory to identify critical assets' challenges. The approach did not provide a systematic process for arriving at criticality decision.

To summarize the literature mentioned above, several contributions use the ML approach in different application domains. However, the comparison results have shown that existing literature has not considered the pressing need to define the various concepts that constitute cybersecurity risk management and how risk prediction can be used within the risk management process. Also, there is little effort in evaluating the effectiveness of existing controls. Therefore, it is necessary to evaluate existing controls so that new controls can be identified and implemented to improve the overall risk management process for CPS. The i-CSRMM is unique in this regard because it conceptualized cybersecurity risk management using a set of concepts from CTI and ML techniques for risk prediction.

#### **6.4.3. Adoption of Industry Standards**

A substantial number of the literature considered for comparison has promoted industry standards to allow consistency and a reliable metric for assessing results' validity. Industry standards generally provide well-documented rules, guidelines, or characteristics for activities and agreement approved by a recognised body that aims to achieve the best degree of order (Saint-Germain, 2005). For example, cybersecurity strategies (tactical, operational and strategic plans) are mapped to security standard such as NIST CSF (Shen, 2014). Furthermore, the authors in ISRAM (Pauley, 2010), NSRM (Ouedraogo and Mouratidis, 2013), (Leitner and Cito, 2016), and ADVISE (Li *et al.*, 2010) have also considered the integration of industry standards in their approach. Most of the literature standards are more security-oriented, meaning they have significant similarity with an i-CSRMM framework in terms of the integration of security standards. However i-CSRMM framework uses a unified approach by focusing on particular sections of renowned standards, guidelines, frameworks and models rather than just security standards. They are applied across different activities within the process by looking at specific features within the standards, frameworks, models and guidelines and where they best fit into the process. For example, NIST CSF tiers have been used for understanding cybersecurity strategy. This is because NIST CSF tiers provide context on how an organisation views cybersecurity risks and the processes in place to manage those risks. CIS CSC have been used for identifying risk control measures. This is because CIS CSC provides 20 controls categorised into three prioritised and defence-in-depth best practices that are implementable to mitigate attacks against systems and networks. Some of these controls are relevant to cybersecurity.

Also, to ensure consistency and relevance of risks and their impact, we adopted the OWASP methodology. OWASP is used for determining the impact of risks because it estimates risks from technical perspectives and business process, and it is highly adaptable and applicable to most organisations of all sizes. In identifying relevant risks, risk sources from OWASP were also considered mainly because it maintained a regularly-updated list of most pressing security concerns and provided a list of 35 risks that fall under categories such as technical, organisational and legal. Also, we integrate some factors from the CWE's common weakness scoring system (CWSS), which provides a mechanism for prioritising software weaknesses in a consistent, flexible, and open manner. It is a standardised approach for characterising weaknesses, thereby allowing organisations to make more informed decisions during the risk management phase and give higher risks. To evaluate the effectiveness of existing controls, we adopt the NIST SP800-30, which enables more effective prioritisation of control actions and decision making because risk assessment requires sufficient threat identification and control, an understanding of threat sources, threat actors behaviour, capability and intent. STIX model is actively being considered for adoption by cyber threat-related organisations, which helps organisations understand the true nature of threats to make intelligent defensive decisions.

#### **6.4.4. Integration of machine learning techniques for i-CSRМ findings on Dataset**

The benefits of machine learning techniques for risk management are still at an early stage. "Reference (Das and Morris, 2017) focused on machine learning techniques for intrusion detection, traffic classification and spam mail protection. However, more analysis needs to be performed to ascertain the algorithms' performance to quantitatively measure the level of cyber-security risks and help critical infrastructure organisations select appropriate controls". In (Livadas et al., 2006), the use of machine learning-based classification techniques, "Naïve Bayes (N.B.)" and "Bayesian belief networks (BBN)" to identify the "command and control (C2)" of botnet-based attack being used as part of a cyber-attack is presented. This approach only considered two different machine learning algorithms, which heavily depended on the training sets and may not be desired in some instances, like risk identification. In (Abu-Nimeh et al., 2007), a study that compares the predictive accuracy of six machine learning classifiers for predicting phishing email is presented. "Reference (Barreno et al., 2010) presented a taxonomy for identifying and analysing attacks against machine learning systems. The problem with this taxonomy is that it is not desirable in cases where organisations want to forecast security risks level".

Machine learning has distinguished itself as a discriminator of malicious and anomalous cybersecurity events for power grid infrastructure. However, the grid provider requires a comprehensive cybersecurity solution to support stakeholders in assessing vulnerabilities and threats for an effective "cybersecurity risk management (CSRМ)". In (Yang et al., 2013), there is a proposal of an "intrusion detection system

(IDS)” for synchro-phasor systems that detect cyber-attacks but is limited to “man-in-the-middle (MITM)” and “denial of service (DoS)” cyber-attacks against synchro-phasor devices only. The authors (Hadeli et al., 2009) proposed an anomaly detection technique for industrial control systems that extract behaviour patterns of devices from networks and communications assets only. This alone cannot minimise the vulnerabilities associated with modern power systems, threats and risks. Every asset of the power grid system is a potential target for a cyber-attack. In the work of (Beaver, Borges-Hink and Buckner, 2013), they applied multiple learning algorithms to Modbus “return terminal unit (RTU)” data in order to demonstrate an ability to discriminate command and data injection attacks on the “supervisory control and data acquisition systems (SCADA)” of a pure gas pipeline system. (Hink et al., 2014) explored the suitability of machine learning methods as a means of discriminating power system disturbances. This work sought to determine an optimal algorithm that is accurate in its classification such that it can provide reliable decision support to a power system operator. However, further work is still required. However, due to the constant changing of the threat landscape and sophisticated technology used to exploit the attack, this task becomes more challenging.

Our work aims to contribute to risk prediction so that an organisation can undertake necessary control and strategic decision for risk control. The proposed i-CSRSM considers various ML techniques and extracts i-CSRSM features which are relevant for the risk prediction. We use a cyber-attack Dataset to get the data for the features so that ML can predicate the risk type. We finally use PCA for selecting the most relevant features such as Assets and TTP. These features performed well on all the classifiers in predicting seven out of ten risk types. PCA reduces the dimensionality by projecting high dimensional data along a smaller number of orthogonal dimensions. We further figure out that PCA's transforming data can improve some of the classifiers such as NN and NB on all the features. Our initial focus is on i-CSRSM for critical infrastructure. However, any organisation can widely adopt the proposed framework to warn of the intensity of risks. Therefore, the implication of such work is vast. An organisation of any size must understand the existing cybersecurity risks and their prediction. It helps to understand the current security control status and undertakes strategic decisions to improve overall cybersecurity so that critical services can continue with no significant disruption due to cybersecurity risks.

The overall results for the prediction of the different risk types based on the given i-CSRSM features indicated that NB-Multi and DT are the best classifiers because they performed better by predicting seven different risk types such as “Crimeware”, “Cyber Espionage”, “Denial of Service”, “Everything Else”, “Lost and Stolen Assets”, “privilege Misuse” and “Point of Sale” while others predicted six or less. Following the above discussion, we observe that i-CSRSM features (TTP, Assets, Controls and Threat Actor) types could predict risk type. Therefore, as security threats grow, organisations need to identify

cybersecurity threats and its trend and also be able to detect and respond to both known and unknown risks. This supports organisations to determine the proper risk type and implement appropriate controls.

#### **6.4.4.1. Comparison with other study results**

This section compares our approach's results with other study results from the literature to generalize our findings. In (Nguyen and Franke, 2012), an adaptive intrusion detection system is proposed that detects different types of attacks in adversarial network environments. However, the proposed framework needs to be applied to other information security problems. In (Salman *et al.*, 2017), an investigation on detecting and categorizing anomalies is carried out using LR and RF machine learning techniques. The result demonstrates that the RF technique with a feature selection scheme can achieve 99% accuracy with anomaly detection. Much research has been carried out in this domain without identifying risk and imposing appropriate countermeasures against different attacks. In (Yavanoglu and Aydos, 2017), the authors reviewed the most commonly used machine learning algorithms, which are primary tools for analysing network traffic, intrusion detection, DDoS attack detection, web applications, and detecting anomalies. However, detecting risk type is still an ongoing plan. In (Liu, Zhang, *et al.*, 2015), the result demonstrates how and to what extent business details about an organisation can help forecast its relative risk of experiencing different types of data incidents using incident reports collected in the VCDB achieve some level of protection. In (Liu, Zhang, *et al.*, 2015) RF classifier is used to train more than 1,000 incidents taken from the VCDB to predict an organisations network breaches. Our work also used ML techniques in the cybersecurity domain but differentiated them from other existing works with a specific focus on cybersecurity risk prediction. Decision Tree is the best classifier in our case, with 93% accuracy initially and further to 96% using PCA. The reason is that the decision tree can quickly identify the most prominent feature to construct the tree and stop the model's induction before overfitting happens, which gave the better generalization error for the test set. We notice that the accuracy is comparatively lower in our case for all the approaches. One possible reason can be the nature of the data, which is highly imbalanced and sparse. As a future endeavor, we intend to use oversampling and sparsity reduction techniques before applying classification algorithms, which might increase the performance of various models.

#### **6.4.5. Implementation process**

A process provides a systematic set of activities that aim to achieve desired objectives, deliver results and provides outputs (Chang, Kuo and Ramachandran, 2016). A practical implementation guide for any approach to address a problem has been highlighted as a vital success factor for any proposed solution to an existing problem (Gottschalk, 1999). The various studies such as (Nocco and Stulz, 2006), (Lai and A

Samad, 2010), (Siang and Ali, 2012) and (Hudin and Hamid, 2014) have provided the underlying architectural and technical guide for implementation. This shows there is a commonality between the literatures mentioned above with the i-CSRSM framework. However, the process proposed by i-CSRSM is more cybersecurity-oriented. It consists of different activities that organisations can follow for understanding and strengthening their cybersecurity risk management by looking at essential considerations such as identifying roles, identifying vulnerabilities and assessing risks. The process also guides organisations to build a cybersecurity strategy from initiation to complete activities based on the need for continuous validation of its assets' integrity. Also, the process is guided by a variety of leading industry best practices, frameworks, guidelines and standards that are generally applicable to all organisations regardless of size. This implies that the process is all-encompassing in nature, not tailored to a specific critical infrastructure domain but built upon high-level considerations to ensure important cybersecurity risk issues are not entirely missed.

## **6.5. Discussion about case study findings**

Discos' staff observed that the integrated i-CSRSM framework is very obliging and detailed for asset identification, assessing potential vulnerabilities and calculating risk level. It provides a comprehensive and holistic analysis of the critical assets, vulnerabilities and threats, and risk types based on the cyber-attack scenarios relevant to the study context. Based on the studied evaluation, the following observations have been made.

### **6.5.1. Applicability of the Framework on case study**

In terms of the framework's applicability, many assumptions have been made. The activities in the process are both practical and appropriate. The integrated risk management framework lays out the basics for defining critical assets, evaluating their weaknesses and risks, and assessing a business disruption risk. This approach has made stakeholders aware of the possible threats that could impact their critical services and business operations, therefore taking the necessary actions to control threats and risk events from occurring. Furthermore, gaining a better view of Disco's existing risk control practices, evaluating them, and suggesting changes raised overall visibility. Disco's management aimed to move from tier 1 (partial) to tier 2 (risk-informed) by proactively incorporating the integrated risk management framework, prioritising data protection practices, informal exchange of intelligence, including all agencies, and cooperation external stakeholders.

The framework is a comprehensive process that incorporates risk management facets from a systemic viewpoint, including stakeholder research and existing standards, from defining cybersecurity strategy to identifying risk. It assesses how a cyber-attack would affect asset targets, organisational functions,

activities, and other technical aspects of the power grid system. The framework evaluates weaknesses, risks, TTP and monitors machine learning techniques to understand the risk level.

### **6.5.2. Comparison with Existing Study Results**

The outcomes of our case study were compared to those of other research reported in the literature. Compared to other works in the literature, the applied cyber-security risk management framework is a systematic solution. A previous author (Buzdugan, 2020) identified a range of security risks and events through different critical infrastructure domains. The work incorporates specific mitigation steps for critical infrastructures, such as vulnerability assessments and penetration testing approaches; however, this paper's emphasis was not just on vulnerability evaluation but also on how danger can be measured, mitigated, and managed. Because of the interdependency between properties, asset detection and cascading vulnerabilities were not taken into consideration. An earlier paper (Ani, He and Tiwari, 2017) provides a helpful overview of potential response directions for understanding industrial control system protection dynamics in terms of cyber risks, weaknesses, assaults, and impacts on the industrial control system (ICS). The work did not introduce some realistic approach to defining properties, evaluating weaknesses, hazards, and minimising risks; instead, it provided some suggestions. Authors of a previous paper (Andrew, 2020) suggested a risk and threat analysis approach for critical infrastructure that focuses on severe incidents while emphasising critical infrastructure business dependencies. However, no systematic study has been performed to define essential assets and weaknesses specific to such assets or identify the specific chains of events (cascading vulnerabilities). (Kumar *et al.*, 2021) suggested a single risk assessment strategy for a power grid infrastructure in a previous. Danger and vulnerability evaluation and categorising were addressed, but properties were not objectively defined, cascading vulnerabilities were not considered, and controls to reduce the risk were not enforced. The authors of a previous paper (Van Greuning and Bratanovic, 2020) stressed the need for a holistic risk management system that includes all phases of the risk management process; our work reflects this to enhance the CPS's cyber-security. Our analysis quantified danger by first defining sensitive properties, then analysing weaknesses, identifying risks, and finally determining the risk level and applying proper controls, as suggested by the writers of a previous paper Ref. (Yaacoub *et al.*, 2020). In their risk evaluation process, the writers of a previous paper (Xu *et al.*, 2020) listed several threats, including the unintentional usage of compromised information media, the disclosure of classified information, and a lack of understanding. This study described these threats, including human mistakes, power outages, unavailability of power, revenue loss to the power grid, and security breaches. In comparison to the writers of a previous paper (Sridhar, Hahn and Govindarasu, 2012a), who suggested a layered method for assessing risks based on protection, our work evaluated risks cyber-attacks databases, as well as risk level and proper controls. Although the

writers of a previous paper (Sun, Hahn and Liu, 2018) explored a framework for avoiding, detecting, and restoring attacks for protecting CPS, our study presented a mechanism for recognising sensitive properties, evaluating cascading weaknesses, creating cyber-attack scenarios, determining the effect of an attack happening, and providing preventive controls to better protect the CPS.

None of the works provides a structured risk assessment mechanism that defines sensitive assets before evaluating vulnerabilities and emphasising the initial vulnerability impact that contributes to the cascading vulnerability effect. Our research identifies and contrasts current risk reduction solutions for CPS in critical infrastructure, allowing critical infrastructure organisations to do an in-depth cyber-security study on CPS. There are certain similarities between our research and other works in terms of risk assessment and reduction. In a previous paper (Bialas, 2016b), the writers discussed danger by addressing interdependencies and risk monitoring. These results are fully or partially close to what we observed in our study. However, specific threats found (Gai *et al.*, 2016), such as energy waste and deploying mobile cloud computing problems, are not strictly comparable to our studied background. Lack of contingency planning, emergency response, reporting systems, robust risk assessment, and the use of machine learning tools to assess the risk level and analyse the efficacy of current controls are some of the specific risk factors not listed in other reports. We urged consumers and operators not to shirk their IT obligations, since the threats of essential infrastructure vary depending on the organization's background. It is also important to raise knowledge of cyber security threats through the whole enterprise and the supply chain climate, as well as to continue to improve and use innovative cyber security capabilities to exercise risk assessment and risk evolution.

### **6.5.3. Study Limitation and Validity**

Some of the participants' observations was that it is difficult to understand the machine learning algorithms for predicting risk type. Also, we tried to reduce the bias of our study finding by actively involving the staff throughout the process. Data was collected from various sources such as interviewing participants, reviewing the existing documentation, and the organisation's internal and external context. The active participation of key staff of the organisation also supported the precondition for action research. However, there is a possibility of cultural bias as data was gathered from a single geographical location. We compared our findings with other study results and observed several common and unique issues to generalize our findings to mitigate this.

## **6.6. Integrating CTI with i-CSRMs findings**

The integration of CTI with the CSRMs helps the studied organisation understand the risk's likelihood and the risk for functional risk calculation. This research's novel contribution is to provide new insights into the effect of cybersecurity by incorporating CTI concepts to improve risk management in critical infrastructure and discover the existence of unknown threats, fully understanding and mitigating those threats to avoid risk to the entire organisation in a proactive manner.

### **6.6.1. Applicability of CTI for improving i-CSRMs**

We have applied a real case study to demonstrate the applicability of this research. The proposed framework is tailored to how CTI improves i-CSRMs for critical infrastructure. It provides a detailed analysis of threat and threat actors profile, existing risk management practice, and controls effectiveness. A brief description of the scenario allows us to exemplify the integration of CTI to improve i-CSRMs in a critical infrastructure. Applying the concepts supports the organisation to have information such as the TTP, incidents, indicators, and the threat actors profile to perform an adequate risk assessment. Having CTI information about threats helps to manage risks effectively, provides mechanisms to prioritise efforts and focus on the most significant risks first. If information about what vulnerabilities are being exploited is known, it can be actively exploited to help decide which security patches should be applied first. The threat information can then be leveraged to help draw a clearer understanding of the risks that the threat environment poses to the organisation.

Furthermore, CTI gave them early warning of potential threats to consider specific operational and tactical decisions to address the threats and associated risks. Also, by setting up a CTI as part of the risk management process, it is assumed that all indicators of compromise are shared, driving towards a better and more informed response to security incidents. It also enables a better security investment strategy. In particular, operational, tactical, and strategic plans enabled both long-term and short-term information security planning by focusing on intelligence collection and analysis to understand threat actors' cyber capabilities, plans, and intentions and enable countermeasures. Evaluating the proposed controls' effectiveness is very difficult without a good understanding of the motives, means, and methods of the threats being addressed. Lastly, this research allows actors to carefully examine an attack pattern's existence and understand threats in a cyber-environment; this allows them to monitor security events continuously. The case study results reveal that having CTI as part of risk management allows organisations to know about threats, improving estimating likelihood and impact of risks.

### **6.6.2. The result from the case study**

The risk level generated was calculated using the threat information factors and the asset security goal factors. The risk being medium needed to be materialised immediately. Therefore we identified ten new controls for them; some of the controls already exist but are identified as either ineffective or not sufficient. The controls were checked to determine whether they should be removed or replaced by a more suitable control. The result suggests that DisCos should adopt CTI for improving i-CSR to detect and respond to threats accordingly. With the adoption of CTI, an organisation can defend against current and future threats, which involves understanding the threat actor's attack pattern, location, skills, motivation and intent to make intelligent defensive decisions.

### **6.6.3. Comparison with other work in adopting CTI for risk management**

When comparing the proposed framework with other approaches, we can quickly identify our framework's unique differences. The authors (Boyson, 2014) proposed a research-based capability/maturity model to capture the spectrum of lagging, collective, and best practices associated with threat intelligence. The work in (Borum *et al.*, 2015) highlights strategic cyber intelligence's importance and role to support risk-informed decision-making. However, it only focuses on the strategic level of planning. The author (Abouzakhar, 2013) presented various security threats and incidents on different critical infrastructure domains. The work introduces some security measures, including vulnerability assessment and penetration testing approaches for critical infrastructure; however, having CTI can further effectively help in risk to be assessed, mitigated and controlled. The work in (Ani, He and Tiwari, 2017) offers an insightful review of possible solution paths of understanding the industrial control systems security trends about cyber threats. The work did not implement the use of CTI to assess vulnerabilities, threats and mitigate risks. This author (Caglayan *et al.*, 2012) examines the behavioural patterns of fast-flux botnets for threat intelligence. The Threat Intelligence infrastructure, which was developed explicitly for fast-flux botnet detection and monitoring, enables this analysis but did not explain how risk can be managed and controlled. In (Yadav and Mahajan, 2015) surveys of the risk assessment methods, significant challenges, and controls for various aspects of the smart grid such as SCADA systems and communication networks to address the challenges facing the innovative grid technologies. However, as a provider, smart grids require a comprehensive cybersecurity solution by supporting stakeholders to assess cyber threats by integrating CTI and providing guidelines for effective risk management.

In a dynamic environment like critical infrastructure, it is essential for risk management to have information about threats to assess threats as it continuously changes. Most of the cyber risk results

from challenges in identifying critical threats, assets affected, parties involved, attributed threat actor, nature of compromise, and historically observed TTP used by the threat actor. Based on the case study, other factors influence a successful attack, such as weak passwords, weak firewalls, and operator unawareness. Managing these risks requires the involvement of CTI. We concluded that threats caused by a cyber-attack could be mitigated or controlled using the threat information with existing risk management and by creating more proactive and adaptive mitigation solutions.

### **6.7. Empirical Studies Conclusion**

The application of the case study approach and the empirical research method used in this research has allowed the researcher to conduct an in-depth empirical analysis of a real-life scenario. The adoption of the case-study technique has enabled the researcher to make systematic observations, collect and analyse data, and establish findings within the context in which activities took place. It also allowed the researcher to observe the complexities of real-life situations, which may not otherwise be captured through other forms or methods. Many participants from two different companies took part in the implementation and determining the validity of the research. The participants provided invaluable feedback on their experiences and perception of the proposed framework. The analysis of the participants' feedback provided an encouraging finding that shows the validity, relevance and acceptability of the proposed framework amongst organisations. The participants expressed optimism about the i-CSRSM framework and its potentiality in addressing the current and emerging cybersecurity issues in critical infrastructure.

### **6.8. Summary**

This chapter discusses the empirical evaluation of the i-CSRSM framework. The chapter provides a detailed discussion regarding empirical studies for validating this research using a case study approach. The evaluation results showed that the i-CSRSM framework provides a comprehensive approach to managing risk in critical infrastructure. The above discussion shows that the underlying activities within the i-CSRSM process were easy to follow, implying that it has a reasonable degree of practicality and usability.

The questionnaire technique enabled feedback collection from participants who took part in the evaluation of i-CSRSM and i-CSRMT to establish the proposed framework's validity, acceptability, and relevance. The chapter also presented results from the case-study contexts. Stakeholder feedback was collected and used to evaluate their perception and view regarding the framework's validity and acceptability. The stakeholders expressed confidence and reasonable satisfaction. The results proved that the proposed framework is highly relevant for helping organisations attain overall cybersecurity risk management. The chapter also compared the literature between some of the critical approaches to risk

management in critical infrastructure. The comparison parameters have been defined based on which the i-CSR framework could be compared against the selected literature. The comparison parameters are created according to the distinct features or contributions of i-CSR. The results of the comparison have shown that the research has made notable contributions to the knowledge domain.

## CHAPTER SEVEN

### CONCLUSION AND FURTHER RESEARCH

#### 7.1. Introduction

Critical infrastructures are increasingly facing many challenges, including cyber-security attacks that tend to disrupt the continuity of its operations and services. The i-CSRSM framework for critical infrastructure is proposed to systematically analyse the risks and offer plans to control the risks to ensure continuity. Every critical infrastructure should implement an effective risk management process that protects it from financial, organisational and reputational loss.

This thesis contributes to the existing literature by providing an i-CSRSM Framework for critical infrastructure to highlight significant risk areas and implement appropriate controls. This helps the critical infrastructure develop foundational knowledge of risk management, integrate the concepts within organisational settings to advocate the creation of cybersecurity risk management awareness, the importance of CTI for improving i-CSRSM and the use of machine learning techniques for risk prediction. To demonstrate the work's applicability, we applied the proposed framework to a power grid CPS and a healthcare system. The case study shows that the framework sufficiently supports the organisation to analyse its security issues, identify critical assets, and assess vulnerabilities and potential threats. Also, to determine risk level, predict risk types and implement the appropriate controls to mitigate those risks. Finally, the i-CSRSM framework provides a critical infrastructure to evaluate the effectiveness of the existing controls. The proposed i-CSRSM framework and i-CSRMT have been validated using real-environment study contexts. Furthermore, the feedback has been collected and analysed to establish the acceptability, relevance, usability and validity of the proposed framework.

To conclude this thesis, this Chapter presents concluding remarks of the fundamental research. It expands how the research objectives could be met, expatriate research contributions to knowledge, and highlights limitations and future research directions.

#### 7.2. Fulfilling Research Objectives

The proposed CSRSM framework has been developed and validated using two real-life case study to meet the research aim: to develop an integrated Cybersecurity Risk Management (i-CSRSM) framework for critical infrastructure protection and resilience *used by organisations that provide essential services for a practical risk assessment*. To ensure the research aim above is satisfied, the objectives were specified as:

- **Objective 1:** To develop an integrated i-CSRSM framework that adopts theoretical concepts to improve the overall CSRSM process to protect critical infrastructures. The framework proposes an implementable process for i-CSRSM activities based on existing industry standards, frameworks and models. The process includes evaluating the effectiveness of existing controls and recommending new control actions in areas where security improvement is needed to protect their systems from potential cyber-security risks and threats. To investigate the usability of the framework, we use different critical organisation domains.
- **Objective 2:** Integration of techniques such as machine learning for risk prediction and accurate information about the risk impact level.
- **Objective 3:** Develop a dedicated integrated cybersecurity risk management tool (i-CSRMT) that automates the overall i-CSRSM process enabling organisations to continuously identify and quantify risks within a reasonable amount of time.

The three main research objectives listed above must be checked to determine whether they are accomplished in the research process. The research has strived to ensure they are completed and an attempt has is made to justify how the objectives are achieved.

### **7.2.1. Develop a Novel Framework**

The research's primary objective entails developing the proposed i-CSRSM framework, which is also necessary for achieving the final research aim. Objective One was accomplished in Chapter Four and Chapter Five. On the one hand, Chapter Two provided the basic principles, background knowledge and understanding of risk management and cybersecurity. Chapter Two contains an analysis of the existing literature in the subject domain. It seeks to identify the critical factor affecting the cybersecurity of critical infrastructures. We reviewed different risk management approaches adopted by the various critical infrastructures for managing cybersecurity risks. Therefore, in Chapter Four, we proposed the framework considering the principles and background knowledge introduced and discussed in Chapter Two. The Chapter started with the unified approach adopted for the proposed i-CSRSM framework that establishes and understands the various concepts that constitute the i-CSRSM framework for critical infrastructure. As it is a highly recommended and common practice to build any framework of relevance based on established theory or methodology, a novel agent-oriented software methodology called Secure Tropos (Mouratidis and Giorgini, 2007) was chosen to develop these concepts. Secure Tropos covers software development from initial requirement analysis and uses concepts such as actors, constraints, and goals. The concepts in Secure Tropos are extended with new concepts such as TTP and Incident to develop for the framework.

Also, the threat landscape is evolving rapidly with new techniques and more sophisticated attacks. The security strategies for mitigating and eliminating these threats are not always enough. We considered CTI to provide comprehensive information about security threats, and this effectively supports i-CSRMM framework activities. Organisations need to integrate CTI with risk management to allow faster detection and alerting of attacks on their assets. Every organisation should implement an effective risk management process with CTI feeds to protect the actors from financial loss, privacy violations, and reputational damage. Our work contributes to the existing literature by providing a unified approach that uses CTI to improve CSRMM. To demonstrate the work's applicability, we applied the proposed framework to a power grid (DisCos). The result shows that the framework sufficiently supports the organisation to analyse their security issues, identify asset goals, assess vulnerabilities and potential threats, and identify risk levels with proper controls to mitigate risks. We advocate for creating i-CSRMM awareness within all organisational levels; staff must not ignore their IT responsibilities.

### **7.2.2. Proposed i-CSRMM process**

Part of objective one aimed at proposing an implementable unified process for the framework activities considering existing risk management standards that provide guidelines to organisations in attaining cybersecurity. There are existing processes for risk management (PatéCornell et al., 2018); however, such techniques have certain limitations because they are not explicitly developed, focusing on or emphasizing risk prediction using CTI information. To fulfill this objective and address the gap, the research attempted to collect systematic activities that produce different outcomes and ensure that the proposed i-CSRMM Framework can be applied to real-world settings. The objective is met in Chapter Five, in which various distinct activities are introduced that guide organisation in attaining cybersecurity from start to finish based on the artifacts of the CSRMM framework as proposed in Chapter Four. The activities consist of essential exercises that range from: determining cybersecurity strategy, analysing the organisational context, identifying and classifying critical assets, identifying vulnerabilities on the assets, identifying threats affecting the assets, performing risk prediction, and determining the effectiveness of existing controls. All these activities and others are combined to create a process for implementing the CSRMM framework. Fundamentally, to ensure adaptability and diverseness, the activities are designed in consideration and by following an assortment of industry best practices, guidelines and standards that are generally applicable to all types of organisations regardless of size or industry. Section 3.2 of the Chapter presented a Unified Approach for the i-CSRMM framework process wherein the sections taken from industry standards, best practices and guidelines used in forming the activities are presented. The risk management activity considered the STIX model and ATT&CK Framework (Barnum, 2012); OWASP; ENISA (ENISA, 2009); and CIS CSC for developing threats profile and risk register respectively. NIST

SP800-30 supports risk response decisions at the different tiers of the risk management hierarchy and ISO 27005:2011 to effectively evaluate controls.

### **7.2.3. Integration of techniques for the prediction of unknown risk and risk level**

Objective two proposed a novel approach for risk prediction using ML techniques. This was accomplished in Chapter Four. The research considers the binary model and trains the ML classifier using the CSRM features. We achieved an accuracy level of 93% initially from the experiment and further improved to 96% by transforming the PCA features. For hybrid algorithms, the order of the best classifiers was found to be NB >> KNN>> LR>>NB Multinomial >> RF >>DT for all the features. Experimental results revealed that decision tree-based algorithms (DT and RF) are well suited for the risk prediction problem (provided they are early pruned to avoid over-fit). This risk prediction can give the organisations an early warning about the risk so that appropriate control can be undertaken proactively. Both industry and research communities have widely recognized ML for its applicability in the cybersecurity domain. However, ML integration for i-CSRM is still early stage, and to the best of our knowledge, this research is one of the first attempts that propose the ML framework for risk type prediction. The primary hypothesis of the study is that we can automate the risk prediction based on occurring events. We use the VCDB dataset and found out that the decision tree provided better accuracy in predicting the risk type.

### **7.2.4. To evaluate the effectiveness of existing controls as well as recommending new control actions in areas where security improvement is needed to protect their systems from any potential cybersecurity risk and threat**

This part of objective one has been accomplished in Chapter five and Chapter seven. An assessment of the existing controls is carried out to ensure the controls are working correctly in mitigating current and future risks. Those controls that do not work correctly were detected, and new controls were implemented.

### **7.2.5. Develop i-CSRMT**

This objective is fulfilled in Chapter six. Objective three aimed at developing an assessment tool that enables organisations to assess their critical assets, identify vulnerabilities and threats, calculate risks levels and evaluate the effectiveness of their existing controls so that informed decisions can be implemented. The primary objective of i-CSRMT is to facilitate the collection of threats and analysis of risks, including the establishment of subjective judgment and determination of the required course of actions that needs to be taken, thereby promoting cybersecurity in critical infrastructures. The objective is drawn by considering the limitations associated with existing works, approaches and tools that have been

designed to foster risk management. Current literature efforts that identify and analyse the risks for organisations mainly consider the analysing risk level. There are complexities involved in the overall risk management process, specifically identifying and quantifying the risks. It requires a reasonable amount of effort for doing the activities under the risks management process. Based on the above context, Chapter six has successfully designed and implemented a proposed i-CSRMT (integrated Cyber Security Risk Management Tool) built to serve as a supporting platform that automates the i-CSRMT process within critical infrastructure. The tool helps to minimise the efforts required to perform the risk management activities and provide accurate information about the risks. Section 6.6 provided a detailed overview of the features supported by i-CSRMT, which are included in the central dashboards: the administrative and actor dashboards.

### **7.2.6. Validate i-CSRMT in real-life critical infrastructure sectors**

Part of objective one is fulfilled in chapter 5. Once the i-CSRMT framework had been developed, it is important to validate it to aid an appropriate case study. A case study and a dataset in a real-life context were selected to evaluate the applicability and the usability of the i-CSRMT framework to enhance risk management in critical infrastructures. The case study allowed for the assessment of the i-CSRMT framework in great detail. The validation result supports the view that the i-CSRMT framework can be applied in any critical infrastructure domain to measure risks effectively. The i-CSRMT framework provides the stakeholders with substantial justification about the risk level to enhance cybersecurity and improve overall risk management, increasing the critical infrastructure's integrity.

Secondly, this objective found out that the i-CSRMT framework is effectively integrated into critical infrastructure domains. Upon applying the i-CSRMT framework, this research found that the unified i-CSRMT process is understood in many ways and applied according to the critical infrastructure domain and its need. Thus, it seems that the i-CSRMT framework can be used for assessing risk controls of high complexity and be customised according to the organisation's objectives. The organisation's stakeholders can quickly learn and use the i-CSRMT framework; the only prerequisite is the basic knowledge of risk management and selecting the cybersecurity tier. The stakeholders who integrated the i-CSRMT framework were satisfied with the outcome as it accelerates the decision-making process and highlights essential risks areas.

### **7.3. Research Limitation**

- Time constraints allowed for only one organisation to be investigated in this research. Also, the risk monitoring activities and residual risks were not thoroughly explored due to the

organisation's lack of time. However, unfulfilled research activities are considered for future research and described in the following section.

- Another limiting factor to be noted for this research is the empirical evaluation method that covered only one case-study. The evaluation part of i-CSRSM enabled the researcher to collect, and analyses feedback from stakeholders' perception and acceptability of the proposed framework. The limited number of case-studies used and responses collected could potentially impact the research's generalisation. The findings would have been generalised if more case study had been covered.
- During the implementation of the i-CSRSM framework, some issues such as human error due to some stakeholders, misunderstanding of the procedures were unfolded. Precisely, some of the framework's activities, such as evaluating the effectiveness of existing controls, are carried out manually without automated techniques. However, the researcher's involvement curtailed this problem; but, it could be a potential issue when adopted.
- The target recipients of this proposed framework are organisations of all size, especially small and medium-sized, the scalability and adaptability of the framework to accommodate diverse and changing environments like that of large organisations who have complex systems and immense requirements is not performed. Therefore, there is a need to apply the research to a large organisation's context to establish its suitability to adapt to diverse contexts.

#### **7.4. Further Research**

During the research process of the i-CSRSM framework, some limitations and difficulties were identified. This research has revealed the potentials for different research directions and works in the area of risk management. It is essential to outline future research and how some of the limitations mentioned above can be addressed.

- One of the participants' observations was that it is difficult to understand the machine learning algorithms for predicting the risk level and risk type. Therefore, we plan to automate the whole i-CSRSM framework process as future research. Full automation of the process will ensure that every activity is performed consistently and accurately and reduces human error chances. Also, it will provide time-saving by reducing the time and the number of personnel required to undertake each activity. Further, the i-CSRSM process automation will improve reliability, thereby leading to wider acceptability amongst critical infrastructures.

- The evaluation of the i-CSRSM framework was performed in a proportionately medium-sized case-study context. Nevertheless, there is a need for further validation in larger-scale situations. Therefore, a potential research area is adjusting and applying the proposed framework to large-scale scenarios to test its efficacy to address critical infrastructures cybersecurity needs. We plan to use the proposed framework in another case study to generalise our findings and validate the framework's applicability.
- The i-CSRSM framework focuses only on the supervised learning method, which requires an existing labelled dataset. As a part of our future research, we will apply unsupervised learning (clustering) to handle the zero-day attacks and use natural learning processing (NLP) for feature extraction. Furthermore, we would like to build an ontology of different risk events and based on the events' semantics, we hope to increase the accuracy of the proposed models further.
- The analysis conducted for this research reveals that the framework continues to be updated and improved as it provides feedback on implementation. As the framework is put into practice, lessons learned will be integrated into future evaluations. This will ensure it meets critical infrastructure owners and operators' needs in a dynamic and challenging environment of new threats, risks, and solutions. In this case, there is room for more research to implement the i-CSRSM framework and update its findings
- As seen in the evaluation of the results, the i-CSRSM framework was designed to be extended to adapt to a dynamic environment. Such an extension can be considered in future work by incorporating more variables to adjust to cyber-attack scenarios.
- As CPS are becoming more complex due to the expansion of businesses and networks, technologies are changing, the coverage of the i-CSRSM framework may have to be customised to suit the Big Data environment, particularly in analysing other forms of data, examining correlations, and establishing predictions for the critical infrastructure.
- Regarding time efficiency to complete the risk management task, i-CSRSM is constrained by the complexity and size of the critical infrastructure and the number of practical control evaluations. Future work should more rigorously examine these consequences by creating a thorough control list and creating a sub-team to test the controls on each critical infrastructure aspect separately.

## 7.5. Summary

Risk management is a continuous process of maintaining the effective functioning of critical assets in any circumstance. The threat landscape is evolving rapidly with new techniques and more sophisticated attacks, and the security strategies for mitigating and eliminating these threats are not consistently

enough. Therefore, risk management's significance is expanding even more, every day as critical infrastructure is becoming more complex, and cybersecurity risks are growingly affecting critical infrastructures. This research proposes an i-CSRMM framework that determines the impact of vulnerabilities on the asset and how they can cascade and result in a more significant issue if not addressed on time. Risk types are analysed using a predictive model influenced by the vulnerabilities identified, threat investigated, TTP used, and IOC of the organisation to provide accurate risk levels. The results of the risks management were integrated into the study context. The proposed framework is demonstrated using the power grid critical infrastructure. An integrated cyber-security risk management framework for the CPS of critical infrastructure can systematically analyse the risks and offer plans to control the risks to ensure business continuity. We believe that the proposed i-CSRMM framework, its process and supporting tool will significantly impact the cybersecurity domain and state of the art in general.

## References

- Aakaash, N. *et al.* (2021) 'Prediction of Network Attacks Using Connection Behavior', in *Machine Learning for Predictive Analysis*. Springer, pp. 299–312.
- Abouzakhar, N. (2013) 'Critical infrastructure cybersecurity: A review of recent threats and violations', in *European Conference on Information Warfare and Security, ECCWS*, pp. 1–10.
- Abu-Nimeh, S. *et al.* (2007) 'A comparison of machine learning techniques for phishing detection', in *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit*, pp. 60–69.
- Abu, M. S. *et al.* (2018) 'Cyber threat intelligence—issue and challenges', *Indonesian Journal of Electrical Engineering and Computer Science*, 10(1), pp. 371–379.
- Adar, E. and Wuchner, A. (2005) 'Risk management for critical infrastructure protection (CIP) challenges, best practices & tools', in *First IEEE International Workshop on Critical Infrastructure Protection (IWCIP'05)*. IEEE, p. 8 pp.
- Addison, T. and Vallabh, S. (2002) 'Controlling software project risks: an empirical study of methods used by experienced project managers', in *Proceedings of the 2002 annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology*. South African Institute for Computer Scientists and Information Technologists, pp. 128–140.
- Ahmed, N. and Abraham, A. (2015) 'Modeling cloud computing risk assessment using machine learning', in *Afro-European Conference for Industrial Advancement*. Springer, pp. 315–325.
- Albladi, S. M. and Weir, G. R. S. (2020) 'Predicting individuals' vulnerability to social engineering in social networks', *Cybersecurity*, 3(1), pp. 1–19.
- Alcaraz, C. and Zeadally, S. (2015) 'Critical Infrastructure Protection: Requirements and Challenges for the 21st Century', 8, pp. 5366–1.
- Alhanahnah, M. J., Jhumka, A. and Alouneh, S. (2016) 'A multidimension taxonomy of insider threats in cloud computing', *The Computer Journal*, 59(11), pp. 1612–1622.
- Alidoosti, A. *et al.* (2012) 'Risk assessment of critical asset using fuzzy inference system', *Risk Management*, 14(1), pp. 77–91.
- Almoghathawi, Y., González, A. D. and Barker, K. (2021) 'Exploring Recovery Strategies for Optimal Interdependent Infrastructure Network Resilience', *Networks and Spatial Economics*, 21(1), pp. 229–260.
- Alqahtani, H. *et al.* (2020) 'Cyber intrusion detection using machine learning classification techniques', in *International Conference on Computing Science, Communication and Security*. Springer, pp. 121–131.

- Amaratunga, D. *et al.* (2002) 'Quantitative and qualitative research in the built environment: application of "mixed" research approach', *Work study*.
- Amin, S. M. (2011) 'Smart grid: Overview, issues and opportunities. advances and challenges in sensing, modeling, simulation, optimization and control', *European Journal of Control*, 17(5–6), pp. 547–567.
- Andrew, L. (2020) 'The vulnerability of vital systems: how 'critical infrastructure' became a security problem', in *Securing 'the Homeland'*. Routledge, pp. 17–39.
- Ani, U. P. D., He, H. (Mary) and Tiwari, A. (2017) 'Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective', *Journal of Cyber Security Technology*. doi: 10.1080/23742917.2016.1252211.
- Argaw, S. T. *et al.* (2020) 'Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks', *BMC Medical Informatics and Decision Making*, 20(1), pp. 1–10.
- Argyroudis, S. A. *et al.* (2020) 'Resilience assessment framework for critical infrastructure in a multi-hazard environment: Case study on transport assets', *Science of The Total Environment*, 714, p. 136854.
- Baldoni, R. (2014) *Critical infrastructure protection: threats, attacks, and counter-measures*. Technical Report. Available online: [http://www. dis. uniroma1. it/~ tenace ....](http://www.dis.uniroma1.it/~tenace)
- Barnum, S. (2008) 'Common attack pattern enumeration and classification (capec) schema description', *Cigital Inc*, [http://capec. mitre. org/documents/documentation/CAPEC\\_Schema\\_Descr iption\\_v1](http://capec.mitre.org/documents/documentation/CAPEC_Schema_Description_v1), 3.
- Barnum, S. (2012) 'Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIX)', *Mitre Corporation*, 11, pp. 1–22.
- Barreno, M. *et al.* (2010) 'The security of machine learning', *Machine Learning*, 81(2), pp. 121–148.
- Baskerville, R. L. and Wood-Harper, A. T. (1996) 'A critical perspective on action research as a method for information systems research', *Journal of information Technology*, 11(3), pp. 235–246.
- Beaver, J. M., Borges-Hink, R. C. and Buckner, M. A. (2013) 'An evaluation of machine learning methods to detect malicious SCADA communications', in *2013 12th International Conference on Machine Learning and Applications*. IEEE, pp. 54–59.
- Benbasat, I., Goldstein, D. K. and Mead, M. (1987) 'The case research strategy in studies of information systems', *MIS quarterly*, pp. 369–386.
- Van den Berg, J. *et al.* (2014) 'On (the emergence of) cyber security science and its challenges for cyber security education', in *Proc. NATO STO/IST-122 symposium*.
- Bialas, A. (2016a) 'Risk management in critical infrastructure-Foundation for its sustainablework',

*Sustainability (Switzerland)*, 8(3). doi: 10.3390/su8030240.

Bialas, A. (2016b) 'Risk Management in Critical Infrastructure—Foundation for Its Sustainable Work', *Sustainability*. doi: 10.3390/su8030240.

Bilge, L., Han, Y. and Dell'Amico, M. (2017) 'Riskteller: Predicting the risk of cyber incidents', in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1299–1311.

Borum, R. *et al.* (2015) 'Strategic cyber intelligence', *Information & Computer Security*.

Boudreau, M.-C., Gefen, D. and Straub, D. W. (2001) 'Validation in information systems research: A state-of-the-art assessment', *MIS quarterly*, pp. 1–16.

Boyson, S. (2014) 'Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems', *Technovation*, 34(7), pp. 342–353.

De Bruijne, M. and Van Eeten, M. (2007) 'Systems that should have failed: critical infrastructure protection in an institutionally fragmented environment', *Journal of contingencies and crisis management*, 15(1), pp. 18–29.

Brydon-Miller, M., Greenwood, D. and Maguire, P. (2003) 'Why action research?' Sage Publications.

Burger, E. W. *et al.* (2014) 'Taxonomy model for cyber threat intelligence information exchange technologies', in *Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security*, pp. 51–60.

Burns, R. B. (2000) 'Introduction to research methods . Frenchs Forest'. NSW: Longman.

Buzdugan, A. (2020) 'Review on use of decision support systems in cyber risk management for critical infrastructures'.

Byres, E. J., Franz, M. and Miller, D. (2004) 'The use of attack trees in assessing vulnerabilities in SCADA systems', in *Proceedings of the international infrastructure survivability workshop*.

Caglayan, A. *et al.* (2012) 'Behavioral analysis of botnets for threat intelligence', *Information systems and e-business management*, 10(4), pp. 491–519.

Cardenas, A. *et al.* (2009) 'Challenges for securing cyber physical systems', in *Workshop on future directions in cyber-physical systems security*.

Cárdenas, A. A. *et al.* (2011) 'Attacks Against Process Control Systems: Risk Assessment, Detection, and Response'.

- Cassell, C. and Symon, G. (2004) *Essential guide to qualitative methods in organizational research*. Sage.
- Castro, J., Kolp, M. and Mylopoulos, J. (2002) 'Towards requirements-driven information systems engineering: the Tropos project', *Information systems*, 27(6), pp. 365–389.
- Chakraverty, S., Sahoo, D. M. and Mahato, N. R. (2019) 'Defuzzification', in *Concepts of Soft Computing*. Springer, pp. 117–127.
- Chang, V., Kuo, Y.-H. and Ramachandran, M. (2016) 'Cloud computing adoption framework: A security framework for business clouds', *Future Generation Computer Systems*, 57, pp. 24–41.
- Chen, P. P.-S. (1976) 'The entity-relationship model—toward a unified view of data', *ACM transactions on database systems (TODS)*, 1(1), pp. 9–36.
- Cherdantseva, Y. *et al.* (2016) 'A review of cyber security risk assessment methods for SCADA systems', *Computers & security*, 56, pp. 1–27.
- Chismon, D. and Ruks, M. (2015) 'Threat intelligence: Collecting, analysing, evaluating', *MWR InfoSecurity Ltd*.
- Coffey, A. and Atkinson, P. (1996) *Making sense of qualitative data: Complementary research strategies*. Sage Publications, Inc.
- Committee, R. S. (2010) 'Department of Homeland Security', *DHS Risk Lexicon—2010 Edition*.
- Connolly, J., Davidson, M. and Schmidt, C. (2014) 'The trusted automated exchange of indicator information (taxii)', *The MITRE Corporation*, pp. 1–20.
- Consortium, W. A. S. (2009) 'Web application security consortium threat classification'.
- Conti, M., Dargahi, T. and Dehghantanha, A. (2018) 'Cyber threat intelligence: challenges and opportunities', in *Cyber Threat Intelligence*. Springer, pp. 1–6.
- Cord, O. (2001) *Genetic fuzzy systems: evolutionary tuning and learning of fuzzy knowledge bases*. World Scientific.
- Cordón, O. (2011) 'A historical review of evolutionary learning methods for Mamdani-type fuzzy rule-based systems: Designing interpretable genetic fuzzy systems', *International journal of approximate reasoning*, 52(6), pp. 894–913.
- Creasey, J. and Marvell, S. (2013) 'A complete information risk management solution For ISF members using IRAM and STREAM', *Managing Information Risk*, pp. 1–7.

- Creswell, J. W. and Creswell, J. D. (2017) *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.
- Cybersecurity, C. I. (2014) 'Framework for Improving Critical Infrastructure Cybersecurity', *Framework*, 1, p. 11.
- Dalziell, E. P. and McManus, S. T. (2004) 'Resilience, vulnerability, and adaptive capacity: implications for system performance'.
- Das, R. and Morris, T. H. (2017) 'Machine learning and cyber security', in *2017 International Conference on Computer, Electrical & Communication Engineering (ICCECE)*. IEEE, pp. 1–7.
- Davis, F. D. (1989) 'Perceived usefulness, perceived ease of use, and user acceptance of information technology', *MIS quarterly*, pp. 319–340.
- Denscombe, M. (2008) 'Communities of practice: A research paradigm for the mixed methods approach', *Journal of mixed methods research*, 2(3), pp. 270–283.
- Denzin, N. K. and Lincoln, Y. S. (2002) *The qualitative inquiry reader*. Sage.
- Dittmeier, C. and Casati, P. (2014) 'Evaluating Internal Control Systems: A Comprehensive Assessment Model (CAM) for Enterprise Risk Management', *Altamonte Springs, Florida: The Institute of Internal Auditors Research Foundation*.
- Eisenhardt, K. M. (1989) 'Building theories from case study research', *Academy of management review*, 14(4), pp. 532–550.
- Ellinas, G. *et al.* (2015) 'Critical infrastructure systems: Basic principles of monitoring, control, and security', in *Intelligent monitoring, control, and security of critical infrastructure systems*. Springer, pp. 1–30.
- Elmaghraby, A. S. and Losavio, M. M. (2014) 'Cyber security challenges in Smart Cities: Safety, security and privacy', *Journal of advanced research*, 5(4), pp. 491–497.
- Enache, M. C. (2015) 'Web Application Frameworks.', *Annals of the University Dunarea de Jos of Galati: Fascicle: XVII, Medicine*, 21(3).
- ENISA, C. C. (2009) 'Benefits, risks and recommendations for information security', *European Network and Information Security*.
- Ericsson, G. N. (2010) 'Cyber security and power system communication—essential parts of a smart grid infrastructure', *IEEE Transactions on Power Delivery*, 25(3), pp. 1501–1507.
- Evans, E. (2004) *Domain-driven design: tackling complexity in the heart of software*. Addison-Wesley

Professional.

- Ezell, B. C. (2007) 'Infrastructure Vulnerability Assessment Model (I-VAM)', *Risk Analysis*, 27(3), pp. 571–583.
- Fang, X. *et al.* (2019) 'A deep learning framework for predicting cyber attacks rates', *EURASIP Journal on Information Security*, 2019(1), p. 5.
- Fekete, A. (2011) 'Common criteria for the assessment of critical infrastructures', *International Journal of Disaster Risk Science*, 2(1), pp. 15–24.
- Firoiu, M. (2015) 'General considerations on risk management and information system security assessment according to ISO/IEC 27005: 2011 and ISO 31000: 2009 standards', *Calitatea*, 16(149), p. 93.
- Fossi, M. *et al.* (2011) 'Symantec internet security threat report trends for 2010', *Volume XVI*.
- Fournaris, A. P., Pocero Fraile, L. and Koufopavlou, O. (2017) 'Exploiting hardware vulnerabilities to attack embedded system devices: a survey of potent microarchitectural attacks', *Electronics*, 6(3), p. 52.
- Gai, K. *et al.* (2016) 'Dynamic energy-aware cloudlet-based mobile cloud computing model for green computing', *Journal of Network and Computer Applications*, 59, pp. 46–54.
- Gandhi, R. *et al.* (2011) 'Dimensions of cyber-attacks: Cultural, social, economic, and political', *IEEE Technology and Society Magazine*, 30(1), pp. 28–38.
- George, P. G. and Renjith, V. R. (2021) 'Evolution of Safety and Security Risk Assessment methodologies to use of Bayesian Networks in Process Industries', *Process Safety and Environmental Protection*.
- Ghorbani, A. A. and Bagheri, E. (2008) 'The state of the art in critical infrastructure protection: a framework for convergence', *International Journal of Critical Infrastructures*, 4(3), pp. 215–244.
- Glass, M. K. *et al.* (2004) *Beginning PHP, Apache, MySQL Web Development*. John Wiley & Sons.
- Goodpaster, K. E. (1991) 'Business ethics and stakeholder analysis', *Business ethics quarterly*, pp. 53–73.
- GOST, R. (2009) 'ISO/IEC 31010-2011 Risk management. Risk assessment methods'.
- Gottschalk, P. (1999) 'Implementation of formal plans: the case of information technology strategy', *Long Range Planning*, 32(3), pp. 362–372.
- Van Greuning, H. and Bratanovic, S. B. (2020) *Analyzing banking risk: a framework for assessing corporate governance and risk management*. World Bank Publications.
- Gupta, R. *et al.* (2020) 'Machine learning models for secure data analytics: A taxonomy and threat

- model', *Computer Communications*, 153, pp. 406–440.
- de Gusmão, A. P. H. *et al.* (2018) 'Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory', *International Journal of Information Management*, 43, pp. 248–260.
- Hadeli, H. *et al.* (2009) 'Leveraging determinism in industrial control systems for advanced anomaly detection and reliable security configuration', in *2009 IEEE Conference on Emerging Technologies & Factory Automation*. IEEE, pp. 1–8.
- Hahn, A. *et al.* (2013) 'Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid', *IEEE Transactions on Smart Grid*, 4(2), pp. 847–855.
- Hall, M. and Brown, L. (2001) *Core web programming*. Prentice Hall Professional.
- Hanus, B., Wu, Y. A. and Parrish, J. (2021) 'Phish Me, Phish Me Not', *Journal of Computer Information Systems*, pp. 1–11.
- Hasson, F., Keeney, S. and McKenna, H. (2000) 'Research guidelines for the Delphi survey technique', *Journal of advanced nursing*, 32(4), pp. 1008–1015.
- Hawk, C. and Kaushiva, A. (2014) 'Cybersecurity and the Smarter Grid', *Electricity Journal*. doi: 10.1016/j.tej.2014.08.008.
- Hickson, I. and Hyatt, D. (2011) 'HTML 5', *W3C Working Draft WD-html5-20110525*, p. 53.
- Hink, R. C. B. *et al.* (2014) 'Machine learning for power system disturbance and cyber-attack discrimination', in *2014 7th International symposium on resilient control systems (ISRCs)*. IEEE, pp. 1–8.
- Hudin, N. S. and Hamid, A. B. A. (2014) 'Drivers to the implementation of risk management practices: A conceptual framework', *Journal of Advanced Management Science Vol*, 2(3), pp. 163–169.
- Hurst, W., Merabti, M. and Fergus, P. (2014) 'A survey of critical infrastructure security', in *International Conference on Critical Infrastructure Protection*. Springer, pp. 127–138.
- Husák, M. *et al.* (2018) 'Survey of attack projection, prediction, and forecasting in cyber security', *IEEE Communications Surveys & Tutorials*, 21(1), pp. 640–660.
- Huyghue, B. D. (2021) 'Cybersecurity, Internet of Things, and Risk Management for Businesses'. Utica College.
- Islam, S. *et al.* (2017) 'A risk management framework for cloud migration decision support', *Journal of Risk and Financial Management*, 10(2), p. 10.

- Ivanenko, O. (2020) 'Implementation of risk assessment for critical infrastructure protection with the use of risk matrix', *ScienceRise*, (2), pp. 26–38.
- Izuakor, C. and White, R. (2016) 'Critical Infrastructure Asset Identification: Policy, Methodology and Gap Analysis', in *Critical Infrastructure Protection X: 10th IFIP WG 11.10 International Conference, ICCIP 2016, Arlington, VA, USA, March 14-16, 2016, Revised Selected Papers 10*. Springer, pp. 27–41.
- Jalali, M. S. and Kaiser, J. P. (2018) 'Cybersecurity in hospitals: a systematic, organizational perspective', *Journal of medical Internet research*, 20(5), p. e10059.
- Jasmin Harvey and Service, T. I. (2007) 'Introduction To Managing Risk', p. 12.
- Jenkins, B. (1998) 'Risk Analysis helps establish a good security posture', *Risk Management keeps it that way, Countermeasures. Inc.*
- Johnson, R. E. and Foote, B. (1988) 'Designing reusable classes', *Journal of object-oriented programming*, 1(2), pp. 22–35.
- Kaplan, B. and Duchon, D. (1988) 'Combining qualitative and quantitative methods in information systems research: a case study', *MIS quarterly*, pp. 571–586.
- Karahanna, E. and Straub, D. W. (1999) 'The psychological origins of perceived usefulness and ease-of-use', *Information & management*, 35(4), pp. 237–250.
- Keele, S. (2007) *Guidelines for performing systematic literature reviews in software engineering*. Technical report, Ver. 2.3 EBSE Technical Report. EBSE.
- Kemabonta, T. and Kabalan, M. (2018) 'Using What You Have, to Get What You Want—A Different Approach to Electricity Market Design for Local Distribution Companies (DISCOs) in Nigeria', in *2018 IEEE Global Humanitarian Technology Conference (GHTC)*. IEEE, pp. 1–2.
- Kemmis, S., McTaggart, R. and Nixon, R. (2013) *The action research planner: Doing critical participatory action research*. Springer Science & Business Media.
- Kim, K.-D. and Kumar, P. R. (2013) 'An overview and some challenges in cyber-physical systems', *Journal of the Indian Institute of Science*, 93(3), pp. 341–352.
- Kirillov, I. et al. (2011) 'Malware attribute enumeration and characterization', *The MITRE Corporation [online, accessed Apr. 8, 2019]*.
- Knight, S. and Burn, J. (2005) 'Developing a framework for assessing information quality on the World Wide Web.', *Informing Science*, 8.
- Kothari, C. R. (2004) *Research methodology: Methods and techniques*. New Age International.

- Kotzanikolaou, P., Theoharidou, M. and Gritzalis, D. (2013) ‘Interdependencies between critical infrastructures: Analyzing the risk of cascading effects’, in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. doi: 10.1007/978-3-642-41476-3\_9.
- Kozik, R. and Chora??, M. (2013) ‘Current cyber security threats and challenges in critical infrastructures protection’, in *2013 2nd International Conference on Informatics and Applications, ICIA 2013*. doi: 10.1109/ICoIA.2013.6650236.
- Kumar, N. *et al.* (2021) ‘A novel framework for risk assessment and resilience of critical infrastructure towards climate change’, *Technological Forecasting and Social Change*, 165, p. 120532.
- Kure, H. I. *et al.* (2021) ‘Asset criticality and risk prediction for an effective cybersecurity risk management of cyber-physical system’, *Neural Computing and Applications*, pp. 1–22.
- Kure, H. I. and Islam, S. (2019) ‘Assets focus risk management framework for critical infrastructure cybersecurity risk management’, *IET Cyber-Physical Systems: Theory & Applications*, 4(4), pp. 332–340.
- Kure, H. I., Islam, S. and Razzaque, M. A. (2018) ‘An integrated cyber security risk management approach for a cyber-physical system’, *Applied Sciences*, 8(6), p. 898.
- Kure, H. and Islam, S. (2019) ‘Cyber Threat Intelligence for Improving Cybersecurity and Risk Management in Critical Infrastructure’, *Journal of Universal Computer Science*, 25(11), pp. 1478–1502.
- Lai, F. W. and A Samad, F. (2010) ‘Enterprise risk management framework and the empirical determinants of its implementation’.
- Lavanya, N. and Malarvizhi, T. (2008) ‘Risk analysis and management: a vital key to effective project management’, in. Project Management Institute.
- Leita, C. and Dacier, M. (2012) ‘Security of power grids: a European perspective’, in *Cybersecurity in Cyber-Physical Systems Workshop*.
- Leitner, P. and Cito, J. (2016) ‘Patterns in the chaos—a study of performance variation and predictability in public iaas clouds’, *ACM Transactions on Internet Technology (TOIT)*, 16(3), pp. 1–23.
- Lerdorf, R., Tatroe, K. and MacIntyre, P. (2006) *Programming Php*. ‘ O’Reilly Media, Inc.’
- Leroux, N. and Kaper, S. de (2014) *Play for Java: Covers Play 2*. Manning Publications Co.
- Levin, D. A. (2021) ‘The State of K-12 Cybersecurity: 2020 Year in Review’, *K-12 Cybersecurity Resource Center*.
- Levy-Bencheton, C. and Darra, E. (2015) ‘Cyber security and resilience of intelligent public transport:

good practices and recommendations’.

Lewis, J. A. (2006) ‘Cybersecurity and Critical Infrastructure Protection’.

Lewis, S. (2015) ‘Qualitative inquiry and research design: Choosing among five approaches’, *Health promotion practice*, 16(4), pp. 473–475.

Lewis, T. G. (2019) *Critical infrastructure protection in homeland security: defending a networked nation*. John Wiley & Sons.

Li, A. *et al.* (2010) ‘CloudCmp: comparing public cloud providers’, in *Proceedings of the 10th ACM SIGCOMM conference on Internet measurement*, pp. 1–14.

Lilly, B. *et al.* (2019) ‘Applying Indications and Warning Frameworks to Cyber Incidents’, in *2019 11th International Conference on Cyber Conflict (CyCon)*. IEEE, pp. 1–21.

Liu, Y., Sarabi, A., *et al.* (2015) ‘Cloudy with a chance of breach: Forecasting cyber security incidents’, in *24th {USENIX} Security Symposium ({USENIX} Security 15)*, pp. 1009–1024.

Liu, Y., Zhang, J., *et al.* (2015) ‘Predicting cyber security incidents using feature-based characterization of network-level malicious activities’, in *Proceedings of the 2015 ACM International Workshop on International Workshop on Security and Privacy Analytics*, pp. 3–9.

Livadas, C. *et al.* (2006) ‘Using machine learning techniques to identify botnet traffic’, in *Proceedings. 2006 31st IEEE Conference on Local Computer Networks*. IEEE, pp. 967–974.

Luna, J. *et al.* (2011) ‘A security metrics framework for the cloud’, in *Proceedings of the International Conference on Security and Cryptography*. IEEE, pp. 245–250.

Machado, L., Filho, O. and Ribeiro, J. (2009) ‘UWE-R: an extension to a web engineering methodology for rich internet applications’, *WSEAS Transactions on Information Science and Applications*, 6(4), pp. 601–610.

Mackenzie, N. and Knipe, S. (2006) ‘Research dilemmas: Paradigms, methods and methodology’, *Issues in educational research*, 16(2), pp. 193–205.

Makawana, P. R. and Jhaveri, R. H. (2018) ‘A bibliometric analysis of recent research on machine learning for cyber security’, in *Intelligent Communication and Computational Technologies*. Springer, pp. 213–226.

Malina, M. A., Nørreklit, H. S. O. and Selto, F. H. (2011) ‘Lessons learned: advantages and disadvantages of mixed method research’, *Qualitative Research in Accounting & Management*, 8(1), pp. 59–71.

- Marinos, L. (2016) 'ENISA Threat Taxonomy: A tool for structuring threat information', *ENISA, Heraklion*.
- Markowski, A. S. and Mannan, M. S. (2009) 'Fuzzy logic for piping risk assessment (pfLOPA)', *Journal of loss prevention in the process industries*, 22(6), pp. 921–927.
- Martin, R. A. (2007) 'Common weakness enumeration', *Mitre Corporation*.
- Mateski, M. *et al.* (2012) 'Cyber threat metrics', *Sandia National Laboratories*.
- Mavroeidis, V. and Bromander, S. (2017) 'Cyber threat intelligence model: an evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence', in *2017 European Intelligence and Security Informatics Conference (EISIC)*. IEEE, pp. 91–98.
- Maxwell, J. A. (2012) *Qualitative research design: An interactive approach*. Sage publications.
- Mbanaso, U. M., Abrahams, L. and Apene, O. Z. (2019) 'Conceptual Design of a Cybersecurity Resilience Maturity Measurement (CRMM) Framework', *African Journal of Information and Communication*, 23, pp. 1–26.
- McNeil, A. J., Frey, R. and Embrechts, P. (2015) *Quantitative risk management: concepts, techniques and tools-revised edition*. Princeton university press.
- McQueen, M. A. *et al.* (2005) *Quantitative Cyber Risk Reduction Estimation for a SCADA Control System*. INL/EXT-05-00319, Idaho National Laboratory, CSSC Report, prepared for US Department of Homeland Security.
- McQueen, M. A. *et al.* (2006) 'Time-to-compromise model for cyber risk reduction estimation', in *Quality of Protection*. Springer, pp. 49–64.
- Mikhalevich, I. F. and Trapeznikov, V. A. (2019) 'Critical infrastructure security: alignment of views', in *2019 Systems of Signals Generating and Processing in the Field of on Board Communications*. IEEE, pp. 1–5.
- Mills, G. E. (2000) *Action research: A guide for the teacher researcher*. ERIC.
- Moteff, J. (2005) 'Risk management and critical infrastructure protection: Assessing, integrating, and managing threats, vulnerabilities and consequences', in. DTIC Document.
- Moteff, J., Copeland, C. and Fischer, J. (2003) 'Critical Infrastructures: What Makes an Infrastructure Critical?'
- Moteff, J. and Parfomak, P. (2004) 'Critical infrastructure and key assets: definition and identification', in. DTIC Document.

- Mouratidis, H. and Giorgini, P. (2007) 'Secure tropos: a security-oriented extension of the tropos methodology', *International Journal of Software Engineering and Knowledge Engineering*, 17(02), pp. 285–309.
- Mrabet, H. *et al.* (2020) 'A survey of IoT security based on a layered architecture of sensing and data analysis', *Sensors*, 20(13), p. 3625.
- NERC, C. I. P. (2006) 'Standards as Approved by the NERC Board of Trustees May 2006'.
- Neuman, W. L. (2013) *Social Research Methods: Pearson New International Edition*. Pearson Education Limited.
- Nguyen, H. T. and Franke, K. (2012) 'Adaptive Intrusion Detection System via online machine learning', in *2012 12th International Conference on Hybrid Intelligent Systems (HIS)*. IEEE, pp. 271–277.
- Nocco, B. W. and Stulz, R. M. (2006) 'Enterprise risk management: Theory and practice', *Journal of applied corporate finance*, 18(4), pp. 8–20.
- Noy, N. F. and McGuinness, D. L. (2001) 'Ontology development 101: A guide to creating your first ontology'. Stanford knowledge systems laboratory technical report KSL-01-05 and ....
- O'Rourke, M. (2017) 'Protecting Our Critical Infrastructure', *Risk Management*, 64(10), pp. 3–4.
- Oates, B. J. (2005) *Researching information systems and computing*. Sage.
- Okutan, A., Yang, S. J. and McConky, K. (2018) 'Forecasting cyber attacks with imbalanced data sets and different time granularities', *arXiv preprint arXiv:1803.09560*.
- Onochie, U. P., Egware, H. O. and Eyakwanor, T. O. (2015) 'The Nigeria electric power sector (opportunities and challenges)', *Journal of Multidisciplinary Engineering Science and Technology*, 2(4), pp. 494–502.
- Organization, W. H. and Control, R. for I. T. (2008) *WHO report on the global tobacco epidemic, 2008: the MPOWER package*. World Health Organization.
- Orlikowski, W. J. and Baroudi, J. J. (1991) 'Studying information technology in organizations: Research approaches and assumptions', *Information systems research*, 2(1), pp. 1–28.
- Östlund, U. *et al.* (2011) 'Combining qualitative and quantitative research within mixed method research designs: a methodological review', *International journal of nursing studies*, 48(3), pp. 369–383.
- Ouedraogo, M. and Mouratidis, H. (2013) 'Selecting a cloud service provider in the age of cybercrime', *Computers & Security*, 38, pp. 3–13.

- Ovelgönne, M. *et al.* (2017) ‘Understanding the relationship between human behavior and susceptibility to cyber attacks: A data-driven approach’, *ACM Transactions on Intelligent Systems and Technology (TIST)*, 8(4), pp. 1–25.
- Papernot, N. *et al.* (2016) ‘Towards the science of security and privacy in machine learning’, *arXiv preprint arXiv:1611.03814*.
- Parhizkar, T., Rafieipour, E. and Parhizkar, A. (2021) ‘Evaluation and improvement of energy consumption prediction models using principal component analysis based feature reduction’, *Journal of Cleaner Production*, 279, p. 123866.
- Paté-Cornell, M. *et al.* (2018) ‘Cyber risk management for critical infrastructure: a risk analysis model and three case studies’, *Risk Analysis*, 38(2), pp. 226–241.
- Patel, S. C., Graham, J. H. and Ralston, P. A. S. (2008) ‘Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements’, *International Journal of Information Management*, 28(6), pp. 483–491.
- Pauley, W. (2010) ‘Cloud provider transparency: An empirical evaluation’, *IEEE Security & Privacy*, 8(6), pp. 32–39.
- Piggin, R. S. H. (2013) ‘Development of industrial cyber security standards: IEC 62443 for SCADA and Industrial Control System security’, in *IET Conference on Control and Automation 2013: Uniting Problems and Solutions*. IET, pp. 1–6.
- Posch, P. N. and Nguyen, T. (2012) ‘Risikoidentifikation und Risikoinstrumente im Rohstoffmanagement’, *Controlling & Management*, 56(2), pp. 52–57.
- Purdy, G. (2010) ‘ISO 31000: 2009—setting a new standard for risk management’, *Risk analysis*, 30(6), pp. 881–886.
- Pyle, D. H. (1999) ‘Bank risk management: theory’, in *Risk Management and Regulation in Banking*. Springer, pp. 7–14.
- Rinaldi, S. M., Peerenboom, J. P. and Kelly, T. K. (2001) ‘Identifying, understanding, and analyzing critical infrastructure interdependencies’, *IEEE Control Systems*, 21(6), pp. 11–25.
- Runeson, P. and Höst, M. (2009) ‘Guidelines for conducting and reporting case study research in software engineering’, *Empirical software engineering*, 14(2), p. 131.
- Sahoo, D., Liu, C. and Hoi, S. C. H. (2017) ‘Malicious URL detection using machine learning: A survey’, *arXiv preprint arXiv:1701.07179*.

- Saint-Germain, R. (2005) 'Information security management best practice based on ISO/IEC 17799', *INFORMATION MANAGEMENT JOURNAL-PRAIRIE VILLAGE-*, 39(4), p. 60.
- Salman, T. *et al.* (2017) 'Machine learning for anomaly detection and categorization in multi-cloud environments', in *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)*. IEEE, pp. 97–103.
- Sapori, E., Sciutto, M. and Sciutto, G. (2014) 'A Quantitative Approach to Risk Management in Critical Infrastructures', *Transportation Research Procedia*, 3, pp. 740–749.
- Sapori E, Sciutto M and Sciutto G (2014) 'ScienceDirect A quantitative approach to risk management in Critical Infrastructures', *Transportation Research Procedia*, 3(3), pp. 740–749. doi: 10.1016/j.trpro.2014.10.053.
- Sasaki, R. (2020) 'A Risk Assessment Method for IoT Systems Using Maintainability, Safety, and Security Matrixes', in *Information Science and Applications*. Springer, pp. 363–374.
- Sauerwein, C., Sillaber, C. and Breu, R. (2018) 'Shadow cyber threat intelligence and its use in information security and risk management processes', *Multikonferenz Wirtschaftsinformatik (MKWI 2018)*, pp. 1333–1344.
- Schauer, S. (2015) 'Novel Approaches To Risk And Security Management For Utility Providers And Critical Infrastructures'.
- Sebastiani, F. (2002) 'Machine learning in automated text categorization', *ACM computing surveys (CSUR)*, 34(1), pp. 1–47.
- Selby, R. W. (2007) *Software engineering: Barry W. Boehm's lifetime contributions to software development, management, and research*. John Wiley & Sons.
- Shackel, B. (2009) 'Usability–Context, framework, definition, design and evaluation', *Interacting with computers*, 21(5–6), pp. 339–346.
- Shehod, A. (2016) 'Ukraine Power Grid Cyberattack and US Susceptibility: Cybersecurity Implications of Smart Grid Advancements in the US'. Cybersecurity Interdisciplinary Systems Laboratory (CILL), Massachusetts ....
- Shen, L. (2014) 'The NIST cybersecurity framework: Overview and potential impacts', *Scitech Lawyer*, 10(4), p. 16.
- Siang, L. C. and Ali, A. S. (2012) 'Implementation of risk management in the Malaysian construction industry', *Journal of Surveying, Construction and Property*, 3(1).

- Silverman, D. (2016) *Qualitative research*. sage.
- Singh, B. and Ghatala, M. H. (2012) 'Risk management in hospitals', *International journal of innovation, management and technology*, 3(4), p. 417.
- Singh, S. K. *et al.* (2020) 'Machine Learning-Based Network Sub-Slicing Framework in a Sustainable 5G Environment', *Sustainability*, 12(15), p. 6250.
- Sridhar, S., Hahn, A. and Govindarasu, M. (2012a) 'Cyber-physical system security for the electric power grid', *Proceedings of the IEEE*. doi: 10.1109/JPROC.2011.2165269.
- Sridhar, S., Hahn, A. and Govindarasu, M. (2012b) 'Cyber-physical system security for the electric power grid', *Proceedings of the IEEE*, 100(1), pp. 210–224.
- Stoneburner, G., Goguen, A. Y. and Feringa, A. (2002) 'Sp 800-30. risk management guide for information technology systems'.
- Straub, D., Boudreau, M.-C. and Gefen, D. (2004) 'Validation guidelines for IS positivist research', *Communications of the Association for Information systems*, 13(1), p. 24.
- Strom, B. E. *et al.* (2017) 'Finding cyber threats with ATT&CK-based analytics', *The MITRE Corporation, Bedford, MA, Technical Report No. MTR170202*.
- Sun, C.-C., Hahn, A. and Liu, C.-C. (2018) 'Cyber security of a power grid: State-of-the-art', *International Journal of Electrical Power & Energy Systems*, 99, pp. 45–56.
- Sun, N. *et al.* (2018) 'Data-driven cybersecurity incident prediction: A survey', *IEEE Communications Surveys & Tutorials*, 21(2), pp. 1744–1772.
- Tactic, A. (2017) 'Techniques and Common Knowledge (ATT&CK)'.
- Tanwar, S. *et al.* (2019) 'Machine learning adoption in blockchain-based smart applications: The challenges, and a way forward', *IEEE Access*, 8, pp. 474–488.
- Taylor, J. M. and Sharif, H. R. (2017) 'Security challenges and methods for protecting critical infrastructure cyber-physical systems', in *Selected Topics in Mobile and Wireless Networking (MoWNeT), 2017 International Conference on*. IEEE, pp. 1–6.
- Ten, C. W., Manimaran, G. and Liu, C. C. (2010) 'Cybersecurity for critical infrastructures: Attack and defense modeling', in *IEEE Transactions on Systems, Man, and Cybernetics Part A: Systems and Humans*. doi: 10.1109/TSMCA.2010.2048028.
- Theocharidou, M. and Giannopoulos, G. (2015) *Risk assessment methodologies for critical infrastructure protection. Part II: A new approach*. tech. report EUR 27332 EN, EU Joint Research Centre.

- Thong, J. Y. L. (1999) 'An integrated model of information systems adoption in small businesses', *Journal of management information systems*, 15(4), pp. 187–214.
- Tolubko, V. *et al.* (2018) 'Method for determination of cyber threats based on machine learning for real-time information system', *International Journal of Intelligent Systems and Applications*, 10(8), p. 11.
- Tounsi, W. and Rais, H. (2018) 'A survey on technical threat intelligence in the age of sophisticated cyber attacks', *Computers & security*, 72, pp. 212–233.
- Trigaux, C. *et al.* (2021) 'SARS-CoV-2: impact on, risk assessment and countermeasures in German Eye Banks', *Current Eye Research*, 46(5), pp. 666–671.
- Turner, J. R. and Danks, S. (2014) 'Case study research: A valuable learning tool for performance improvement professionals', *Performance Improvement*, 53(4), pp. 24–31.
- Tweneboah-Koduah, S. and Buchanan, W. J. (2018) 'Security risk assessment of critical infrastructure systems: A comparative study', *The Computer Journal*, 61(9), pp. 1389–1406.
- Tymchuk, O., Iepik, M. and Sivyakov, A. (2017) 'Information security risk assessment model based on computing with words', in *MENDEL*, pp. 119–124.
- Varshney, K. R. and Alemzadeh, H. (2017) 'On the safety of machine learning: Cyber-physical systems, decision sciences, and data products', *Big data*, 5(3), pp. 246–255.
- Veeramachaneni, K. *et al.* (2016) 'AI<sup>2</sup>: training a big data machine to defend', in *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)*. IEEE, pp. 49–54.
- Venkatesh, V. *et al.* (2003) 'User acceptance of information technology: Toward a unified view', *MIS quarterly*, pp. 425–478.
- Virtualization, N. F. (2013) 'European Telecommunications Standards Institute (ETSI)', *Industry Specification Group (ISG)*.
- Walsham, G. (1995) 'Interpretive case studies in IS research: nature and method', *European Journal of information systems*, 4(2), pp. 74–81.
- Wang, S., Zhang, J. and Gan, L. (2016) 'Vulnerability analysis and critical components identification of Power Networks under cascading failures', in *Control Conference (CCC), 2016 35th Chinese*. IEEE, pp. 6570–6574.
- Warkentin, M. *et al.* (2009) 'Analysis of systems development project risks: An integrative framework',

*ACM SIGMIS Database*, 40(2), pp. 8–27.

Wichers, D. (2013) ‘Owasp top-10 2013’, *OWASP Foundation*, February.

Widup, S. (2013) ‘The veris community database’.

Workman, M., Bommer, W. H. and Straub, D. (2008) ‘Security lapses and the omission of information security measures: A threat control model and empirical test’, *Computers in human behavior*, 24(6), pp. 2799–2816.

Wu, W., Kang, R. and Li, Z. (2015) ‘Risk assessment method for cyber security of cyber physical systems’, in *Reliability Systems Engineering (ICRSE), 2015 First International Conference on*. IEEE, pp. 1–5.

Xiong, W. *et al.* (2021) ‘Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix’, *Software and Systems Modeling*, pp. 1–21.

Xu, J. *et al.* (2020) ‘Seismic risk evaluation for a planning mountain tunnel using improved analytical hierarchy process based on extension theory’, *Journal of Mountain Science*, 17(1), pp. 244–260.

Xu, M. *et al.* (2018) ‘Modeling and predicting cyber hacking breaches’, *IEEE Transactions on Information Forensics and Security*, 13(11), pp. 2856–2871.

Xu, M., Hua, L. and Xu, S. (2017) ‘A vine copula model for predicting the effectiveness of cyber defense early-warning’, *Technometrics*, 59(4), pp. 508–520.

Yaacoub, J.-P. A. *et al.* (2020) ‘Cyber-physical systems security: Limitations, issues and future trends’, *Microprocessors and Microsystems*, 77, p. 103201.

Yadav, D. and Mahajan, A. R. (2015) ‘Smart grid cyber security and risk assessment: an overview’, *Int. J. Sci. Eng. Technol. Res*, 4, pp. 3078–3085.

Yan, Y. *et al.* (2012) ‘A survey on cyber security for smart grid communications’, *IEEE Communications Surveys and Tutorials*. doi: 10.1109/SURV.2012.010912.00035.

Yang, Y. *et al.* (2013) ‘Intrusion detection system for network security in synchrophasor systems’.

Yavanoglu, O. and Aydos, M. (2017) ‘A review on cyber security datasets for machine learning algorithms’, in *2017 IEEE International Conference on Big Data (Big Data)*. IEEE, pp. 2186–2193.

Yavneh, A., Lothan, R. and Yamin, D. (2021) ‘Co-similar malware infection patterns as a predictor of future risk’, *PloS one*, 16(3), p. e0249273.

Yin, R. K. (2009) ‘Case study research: Design and methods 4th edition’, in *United States: Library of*

*Congress Cataloguing-in-Publication Data.*

Yoneda, S. *et al.* (2015) 'Risk assessment in cyber-physical system in office environment', in *Proceedings - 2015 18th International Conference on Network-Based Information Systems, NBiS 2015*. doi: 10.1109/NBiS.2015.63.

Zachman, J. A. (1987) 'A framework for information systems architecture', *IBM systems journal*, 26(3), pp. 276–292.

Zadeh, L. A. (1988) 'Fuzzy logic', *Computer*, 21(4), pp. 83–93.

Zimmermann, H.-J. (2011) *Fuzzy set theory—and its applications*. Springer Science & Business Media.

Zografopoulos, I. *et al.* (2021) 'Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies', *IEEE Access*, 9, pp. 29775–29818.

Županović, I. (2014) 'Sustainable Risk Management in the Banking Sector', *Journal of Central Banking Theory and Practice*, 3(1), pp. 81–100.

## Appendices

### Appendix A: Questionnaire Evaluation for Framework Evaluation

#### Acceptability Ratings for the Proposed Framework

The purpose of this questionnaire is to collect your feedback about the proposed “**An Integrated Cyber Security Risk Management Framework for Critical Infrastructure Protection**”, which is aimed at supporting your organisation in achieving and enhancing risk management. Your feedback is critical in establishing the validity of the proposed Framework and areas of improvement. Kindly respond to the questions that follow by “checking” one of the boxes where appropriate. The questions are designed and evaluated according to criterion as:

1. **Ease of use:** inquiries whether the Framework is designed so that users can easily use it.
2. **Relevance:** determines whether the Framework is relevant in terms of feasibility for supporting your organisation achieve cybersecurity risk management.
3. **Usefulness:** whether the Framework will be very useful in helping the organisation achieve cybersecurity risk management.
4. **Flexibility and dynamics:** whether the Framework is dynamic enough to cover and deal with larger contexts and scenarios.
5. **Compliance with security standards and best practices:** attempts to establish whether the Framework complies with industry standards such as ISO27001 and NIST
6. **Trustworthiness:** inquiries whether the Framework is trustworthy in ensuring privacy and security and preventing future cybersecurity issues.

Thank you for your cooperation.

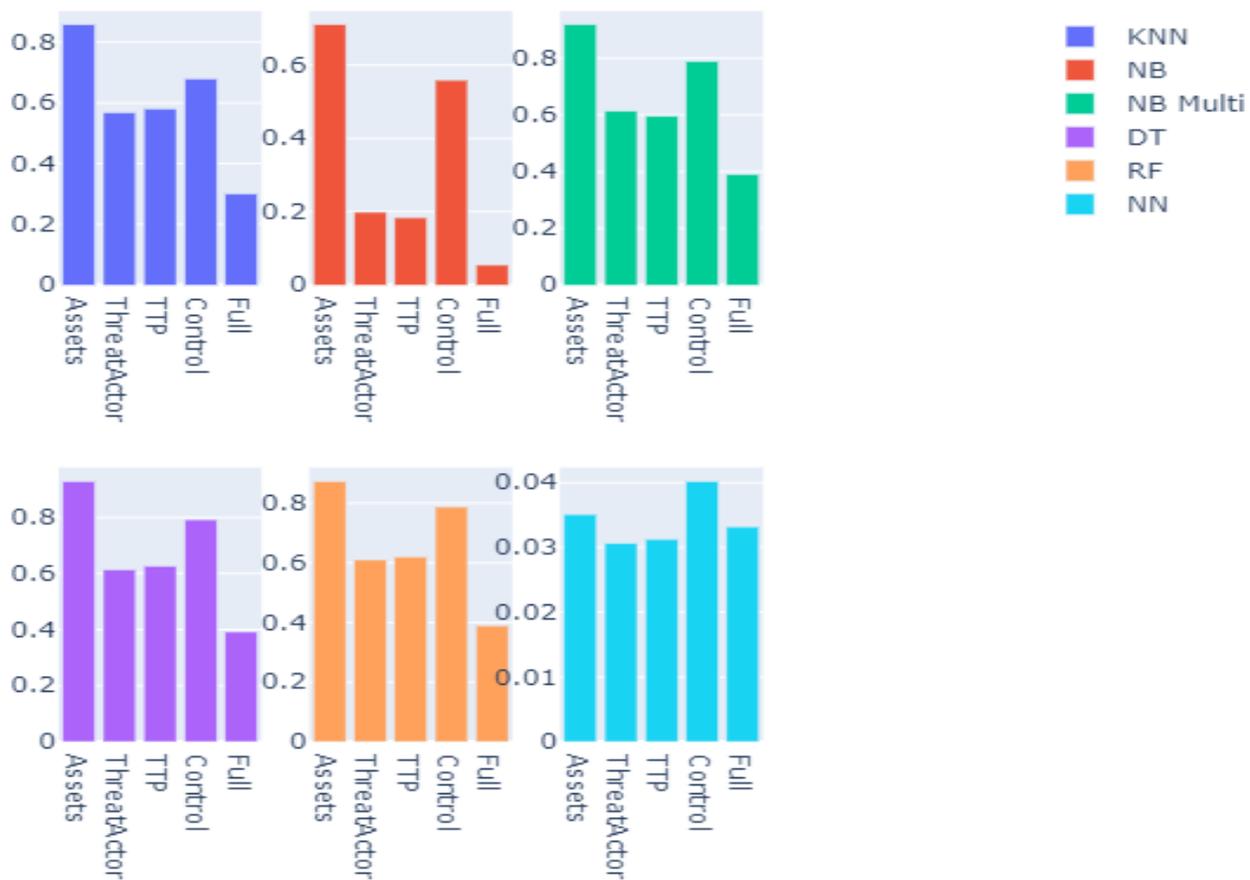
S/N	Evaluation Criteria	Question	Response Options			
			Strongly Agree	Agree	Not Sure	Disagree
1.	Ease of Use	Do you agree that i-CSRMT Framework and i-CSRMT is clear and easily understandable to intended users?				
2.	Relevance	Do you agree that the proposed Framework is relevant for supporting organisations to achieve				

		cybersecurity risk management?				
3.	Usefulness	Do you agree that the proposed Framework is helpful in terms of the expected deliverables?				
4.	Flexibility	Do you agree that the proposed Framework is flexible to adapt to dynamic and complex contexts?				
5.	Compliance with security standards and best practices	Does the Framework comply with relevant laws, standards and best practices?				
6.	Trustworthiness	Do you consider the proposed Framework to be trustworthy in ensuring cybersecurity risk management?				

## Appendix B

### Results of the Training Set

The accuracy results of different classifiers for the various kinds of input features are explained here. The most prominent features to detect the risk type are Assets and Controls where accuracy is above 70%. From left to right (top to bottom), the X-axis denotes different classifiers and Y-axis denotes the corresponding accuracy for a given feature set. It can be seen from the descriptive result is based on the asset features KNN, NB Multi, RF and DT have produced the most accurate predictions by giving the accuracy value of above 70% compared to NB and NN classifiers. The graph's predictive results for control features indicate that DT produced the maximum accuracy with a value of 79% compared to other classifiers. Therefore, DT for Control features is the best predictive classifier. The different algorithms were used to determine the predictive accuracy for Threat Actor features. DT, RF, KNN and NB Multi produced maximum accuracy, however, DT and NB Multi produced the most accuracy (61%). Further, and we checked the performance of the different algorithms under the TTP features. DT, RF, KNN and NB Multi produced good accuracy but DT outperformed other algorithms with 62%. NN and NB algorithms did not give us excellent results. Lastly, the Full feature result in the graph below shows all the classifiers produced accuracy of 39% and less. The result shows that Full features did not perform well on all the classifiers. Therefore, we can conclude that the best algorithm that performed well on all the input features except the full feature is DT and NB Multi.



**Figure AC1:** The accuracy of different classifiers for various types of input binary features on the test

## Appendix C

### Result of the Confusion Matrix for the best classifier (DT).

```
Confusion results are
```

Out[6]:

	precision	recall	f1-score	support
<b>0</b>	0.886792	0.510870	0.648276	92.00000
<b>1</b>	0.730570	0.771335	0.750399	914.00000
<b>2</b>	0.789796	0.732492	0.760065	1585.00000
<b>3</b>	0.582694	0.698621	0.635414	1523.00000
<b>4</b>	0.603219	0.854618	0.707242	1754.00000
<b>5</b>	0.789474	0.280899	0.414365	267.00000
<b>6</b>	0.727891	0.405303	0.520681	264.00000
<b>7</b>	0.925373	0.385093	0.543860	161.00000
<b>8</b>	0.919048	0.784553	0.846491	246.00000
<b>9</b>	0.651838	0.327502	0.435964	1029.00000
<b>accuracy</b>	0.670070	0.670070	0.670070	0.67007
<b>macro avg</b>	0.760670	0.575129	0.626276	7835.00000
<b>weighted avg</b>	0.688629	0.670070	0.657428	7835.00000

Performance measure for the various risk types based on the different features

## Appendix D

### Snippets of the Jaro-Wrinkler Similarity code

```
1 // Jaro Winkler similarity index - Author: Augustine Nawa
2 public function compare($str1, $str2)
3 {
4     return $this->JaroWinkler($str1, $str2, $PREFIXSCALE = 0.1 );
5 }
6
7 private function getCommonCharacters( $string1, $string2, $allowedDistance ){
8
9     $str1_len = mb_strlen($string1);
10    $str2_len = mb_strlen($string2);
11    $temp_string2 = $string2;
12
13    $commonCharacters='';
14    for( $i=0; $i < $str1_len; $i++){
15
16        $noMatch = True;
17        // compare if char does match inside given allowedDistance
18        // and if it does add it to commonCharacters
19        for( $j= max( 0, $i-$allowedDistance ); $noMatch && $j < min( $i + $allowedDistance + 1, $str2_len ); $j++){
20            if( $temp_string2[$j] == $string1[$i] ){
21                $noMatch = False;
22                $commonCharacters .= $string1[$i];
23                substr($temp_string2[$j], 1);
24            }
25        }
26    }
27    return $commonCharacters;
28 }
29
30 private function Jaro( $string1, $string2 ){
31
32    $str1_len = mb_strlen( $string1 );
33    $str2_len = mb_strlen( $string2 );
34
35    // theoretical distance
36    $distance = (int) floor(min( $str1_len, $str2_len ) / 2.0);
37
38    // get common characters
39    $commons1 = $this->getCommonCharacters( $string1, $string2, $distance );
40    $commons2 = $this->getCommonCharacters( $string2, $string1, $distance );
41
42    if( ($commons1_len = mb_strlen( $commons1 )) == 0 ) return 0;
43    if( ($commons2_len = mb_strlen( $commons2 )) == 0 ) return 0;
44    // calculate transpositions
45    $transpositions = 0;
46    $upperBound = min( $commons1_len, $commons2_len );
47    for( $i = 0; $i < $upperBound; $i++){
48        if( $commons1[$i] != $commons2[$i] ) $transpositions++;
49    }
50    $transpositions /= 2.0;
51    // return the Jaro distance
52    return ( $commons1_len/($str1_len) + $commons2_len/($str2_len) + ($commons1_len - $transpositions)/($commons1_len) ) / 3.0;
53 }
54
55 private function getPrefixLength( $string1, $string2, $MINPREFIXLENGTH = 4 ){
56
57    $n = min( array( $MINPREFIXLENGTH, mb_strlen($string1), mb_strlen($string2) ) );
58
59    for($i = 0; $i < $n; $i++){
60        if( $string1[$i] != $string2[$i] ){
61            // return index of first occurrence of different characters
62            return $i;
63        }
64    }
65
66    // first n characters are the same
67    return $n;
68 }
69
70 private function JaroWinkler($string1, $string2, $PREFIXSCALE = 0.1 ){
71
72    $JaroDistance = $this->Jaro( $string1, $string2 );
73    $prefixLength = $this->getPrefixLength( $string1, $string2 );
74    return $JaroDistance + $prefixLength * $PREFIXSCALE * (1.0 - $JaroDistance);
75 }
76
```

### Deriving the Risk Level

```

1 //Deriving the Risk Level - RL = SUM(RLi, AS1) x RIV
2 if(count($this->assets) > 0){
3 //Get the attackers skills level
4 $matchedRL = $this->topMatch['Skills_Required'];
5 if (($pos = strpos($matchedRL, "LEVEL : ") !== FALSE) {
6     $this->AS = substr($matchedRL, $pos+8);
7 }
8
9 //convert AS1 to value
10 if(trim($this->AS) == "Low"){
11     $this->AS1 = 0;
12 }
13 elseif(trim($this->AS) == "Medium"){
14     $this->AS1 = 2.5;
15 }
16 elseif(trim($this->AS) == "High"){
17     $this->AS1 = 5;
18 }
19 }
20 //Get the likelihood of an attack
21 $matchedRLi = trim($this->topMatch['attackLikelihood']);
22
23 //convert RLi to value
24 if($matchedRLi == "Low"){
25     $this->RLi = 0;
26 }
27 elseif($matchedRLi == "Medium"){
28     $this->RLi = 2.5;
29 }
30 elseif($matchedRLi == "High"){
31     $this->RLi = 5;
32 }
33 }
34 //Get the impact value
35 $impactRatingDBP = $impactRatingUCDS = $impactRatingLDIUCA = $impactRatingFPSTAO = $impactRatingIDASAC =
36 $impactRatingDLL = $impactRatingFSSRO = $impactRatingIOCDs = 0;
37
38 foreach ($this->riskImpact as $RM) {
39     if(trim($RM->risk_name) == 'Disruption of business process'){
40         $impactRatingDBP += $RM->impact_rating;
41     }
42     elseif(trim($RM->risk_name) == 'Unavailability of critical data and assets'){
43         $impactRatingUCDS += $RM->impact_rating;
44     }
45     elseif(trim($RM->risk_name) == 'Loss of data integrity and unauthorised changes to assets'){
46         $impactRatingLDIUCA += $RM->impact_rating;
47     }
48     elseif(trim($RM->risk_name) == 'Failure to provide security transparency and accountability by the orgainsation'){
49         $impactRatingFPSTAO += $RM->impact_rating;
50     }
51     elseif(trim($RM->risk_name) == 'Inadequate data and application security, administration and control.'){
52         $impactRatingIDASAC += $RM->impact_rating;
53     }
54     elseif(trim($RM->risk_name) == 'Data loss and leakage'){
55         $impactRatingDLL += $RM->impact_rating;
56     }
57     elseif(trim($RM->risk_name) == 'Failure to satisfy stipulated requirements by the orgainsation'){
58         $impactRatingFSSRO += $RM->impact_rating;
59     }
60     elseif(trim($RM->risk_name) == 'Inability of the orgainsation to meet compliance needs of data and services'){
61         $impactRatingIOCDs += $RM->impact_rating;
62     }
63 }
64
65 //Calculating the RL
66 $this->RLDBP = ($this->RLi + $this->AS1) * $impactRatingDBP;
67 $this->RLUCDS = ($this->RLi + $this->AS1) * $impactRatingUCDS;
68 $this->RLLDIUCA = ($this->RLi + $this->AS1) * $impactRatingLDIUCA;
69 $this->RLFPSTAO = ($this->RLi + $this->AS1) * $impactRatingFPSTAO;
70 $this->RLIDASAC = ($this->RLi + $this->AS1) * $impactRatingIDASAC;
71 $this->RLDLL = ($this->RLi + $this->AS1) * $impactRatingDLL;
72 $this->RLFSSRO = ($this->RLi + $this->AS1) * $impactRatingFSSRO;
73 $this->RLIOCDs = ($this->RLi + $this->AS1) * $impactRatingIOCDs;
74

```

For deriving final risk score

```
1 //Deriving the Risk Status - RS = RL - CS
2 $MIDBP = $MIUCDS = $MLDIUCA = $MIFPSTAO = $MIIDASAC = $MIDLL = $MIFSSRO = $MIOCDs = 0;
3 if($this->riskMitigation){
4     foreach($this->riskMitigation as $mitigation){
5         if(trim($mitigation->risk_name) == 'Disruption of business process'){
6             $MIDBP += $mitigation->risk_value;
7         }
8
9         if(trim($mitigation->risk_name) == 'Unavailability of critical data and assets'){
10            $MIUCDS += $mitigation->risk_value;
11        }
12
13        if(trim($mitigation->risk_name) == 'Loss of data integrity and unauthorised changes to assets'){
14            $MLDIUCA += $mitigation->risk_value;
15        }
16
17        if(trim($mitigation->risk_name) == 'Failure to provide security transparency and accountability by the organisation'){
18            $MIFPSTAO += $mitigation->risk_value;
19        }
20
21        if(trim($mitigation->risk_name) == 'Inadequate data and application security, administration and control.'){
22            $MIIDASAC += $mitigation->risk_value;
23        }
24
25        if(trim($mitigation->risk_name) == 'Data loss and leakage'){
26            $MIDLL += $mitigation->risk_value;
27        }
28
29        if(trim($mitigation->risk_name) == 'Failure to satisfy stipulated requirements by the organisation'){
30            $MIFSSRO += $mitigation->risk_value;
31        }
32
33        if(trim($mitigation->risk_name) == 'Inability of the organisation to meet compliance needs of data and services'){
34            $MIOCDs += $mitigation->risk_value;
35        }
36    }
37
38    //Calculating the final Risk Status
39    $this->RSDBP = $this->RLDBP - $MIDBP;
40    $this->RSUCDS = $this->RLUCDS - $MIUCDS;
41    $this->RSDIUC = $this->RLDIUCA - $MLDIUCA;
42    $this->RSFPSTAO = $this->RLFPSTAO - $MIFPSTAO;
43    $this->RSIDASAC = $this->RLIDASAC - $MIIDASAC;
44    $this->RSDLL = $this->RLD11 - $MIDLL;
45    $this->RSFSSRO = $this->RLFSSRO - $MIFSSRO;
46    $this->RSIOCDs = $this->RLIOCDs - $MIOCDs;
47 }
```

## Appendix E

### Asset Inventory

Table E1 displays the asset inventory showing the critical level for each asset.

**Table E1:** Asset Inventory

Asset Name	Asset Description	Asset Goals					Asset Criticality			
		C	I	A	CON	ACC	Low	Medium	High	Very High

### Threat Profile

Table E2 displays the threat profile showing the output of the threat modelling activity used as an input for the risk assessment activity.

**Table E2: Threat Profile**

Threat Name	Threat Description	Target Asset	Execution Flow	Related Attack Pattern	Possible Vulnerabilities	Threat Actor Factors		Indicator of Compromise	TTP Category
						Skills Required	Resources Required		

## Control Types

Table E3 displays the list of the different controls types.

**Table E3: Control Types**

Control Type	Control Description

## Risk Control Profile

Table E4 displays the control type together with its calculated overall control effectiveness value.

**Table E4: Risk Control Profile**

Control Type	Control Description	Criteria					Overall Control Effectiveness
		S	R	C	I	T	

## Risk Status profile

Table E5 displays the new risk status after controls has been implemented.

**Table E5: Risk status**

Risk Type	Risk Impact Level	Control measures Implemented			Risk Status
		None	Partial	Full	

## Risk Register

Table E6 presents the risk register with the list of the risk types, existing control measures and the risk impact level.

**Table E6: Risk Register**

Risk Name	Risk Likelihood			Risk Impact on Security goals			Control Measures			Risk Value
	Low	Med	High	Low	Med	High	None	Partial	Full	