SWOT Analysis of Information Security Management System ISO 27001

Information Security is considered one of the main concerns for many organisations with no signs of decreasing urgency in the coming years. To address this concern a structured approach required, with the ISO 27000 series - Information Security Management Systems (ISMS) being one of the most popular practices for assessing and managing Information Security. However, assessing the effectiveness of a security management approach in order to further develop it is far from straightforward. Many organisations still do not share information about their security incidents or breaches, while many breaches go unnoticed, making enhancing an ISMS process a challenge. In this work, we used a combination of research methods (interviews and workshops) to conduct a SWOT analysis on ISMS. The findings from the SWOT were then validated using a survey covering auditors, consultants and researchers in the field. Finally, the results were validated and analysed using various statistical methods. Our findings show that there was a generally positive view on the 'Strengths' and 'Opportunities' compared to that of 'Weaknesses' and 'Threats'. We identified statistically significant differences in the perception of 'Strengths' and 'Opportunities' across the groups but also found that there is no significant variance in the perception of 'Threats'. The SWOT produced will help practitioners and researchers tailor ways to enhance ISMS using existing techniques such as TOWS matrix.

Keywords: Information Security Management Systems, Information Security Risk Management, security control framework, IT audit

Author(s):
Iretioluwa Akinyemi, University Of East London
Daniel Schatz, University Of East London, daniel@virturity.com
Rabih Bashroush, University Of East London
Affiliation: University of East London, Docklands Campus, 4-6 University Way, London E16 2RD

1 INTRODUCTION

Information assets are seen as the lifeblood in every business and can be valued by the inputs of the gross domestic product (GDP) attributable to processes and services that are information-related; a loss in information assets has the potential terminate a business (Barlette and Fomin, 2008). Every organization must deal with a variety of risk on a day to day basis, with information security emerging as one of the most important areas (Prislan and Bernik, 2010). Information security deals with safeguarding of information from threats and as such enables organizations to maximize business opportunities safely in context of information risks. Tipton and Krause (2012) state that confidentiality, integrity and availability are information security goals providing assurance for business information. Confidentiality certifies that the data or information owner has the right to gain access to it and ensures confidentiality of data accepted, sent or saved. Integrity on the other hand ensures that information or data cannot be changed except where there is permission to do so. Lastly, the availability property demands that data or information is accessible when needed.

A set of benchmarks or standards are needed to help organizations to attain suitable levels of security to maximize efficient use of resources. ISO 27001 is such a standard and is widely used globally (International Standards Organisation, 2014). The ISO 27001 information security standard is one of the standards in the ISO 27000 series that describes certification and audit requirements of an organization's Information Security Management System (ISMS). The goal of the standard is to establish, implement, operate, monitor, review, maintain and improve an information security management system (Honan, 2010). It originated from a code of good practice that was produced by the UK Department of Trade and Industry in 1989 which then slowly advanced into BS 7799, ISO 17999 and eventually ISO 27001 (Broderick, 2006).

To obtain certification under the standard, an organization must comply with a set of defined requirements. The organisations' ISMS as a whole must be supported by a set of requisites relating to internal audits, management responsibility, documentation, system improvement and management

review (Valdevit and Mayer, 2010). The identification, fulfilment and management of security risks are difficult for many organizations and stakeholders to handle. As such, ISO 27001 becomes a tool or route to proffering solutions to problems of such magnitude. The standard specifies a process for the establishment and maintenance of Information Security Management Systems, which tunes security to the particular need of any kind of organization (Beckers et al., 2014).

However, driving the development and further enhancement of ISMS' is far from straightforward. Many organisations do not share information about their security incidents or breaches. Thus, using common approaches to measure effectives of an intervention, such as comparing the situation before and after an intervention, is difficult to apply in this case making the assessment of ISMS' effectiveness a challenge.

In this study, we propose a Strengths, Weaknesses, Opportunities and Threats (SWOT) analysis as an approach to identify ways to enhance ISMS such as ISO 27001. We conducted SWOT analysis in form of workshops and interviews with qualified auditors, consultants and researchers in the field. The findings of these sessions were then validated using a survey instrument, and the results significance was analysed using statistical methods. In this paper, we report on our findings.

The remainder of the paper is structured as follows. Section 2 introduces the research methodology and discusses how the credibility of the study participants was established. Section 3 covers the literature review, providing background on ISO 27001 and offering a view on other relevant security frameworks. Section 4 presents our findings of the SWOT workshop exercise. Section 5 presents the results and analysis of the survey. In section 6, we discuss the findings and their significance using statistical analysis methods. Then, section 7 lists the limitations of this study. Finally, section 8 rounds off the paper by summarizing the findings and making recommendations for future work.

2 RESEARCH METHODOLOGY

This research proposes SWOT analysis (Hill and Westbrook, 1997) as a way to drive the review and enhancement process of ISMS using the practical example of ISO 27001. A SWOT approach consists of two areas of analysis. The first area addresses the local (internal) factors, which covers discussions on the strengths and weaknesses of the subject being studied (in this case ISMS). The second area addresses the external (global) factors, which covers discussions of the relevant environmental or contextual opportunities and threats.

Accordingly, the following research questions were identified:

RQ.1 What are the Strengths and Weakness of ISMS?

RQ.2 What are the Opportunities and Threats for ISMS?

RQ.3 What is the significance of the findings?

In order to answer the above research questions, a mixed method approach, combining qualitative and quantitative methods (Johnson and Onwuegbuzie, 2004, Creswell, 2013) was used. In first instance, a series of interviews and workshops were conducted with representatives of relevant groups (face to face and phone based). This included certified ISO 27001 auditors, consultants and security researchers (4 of each category, 12 in total, with various years of experience and geographic locations) to gather a consensus on the Strengths, Weaknesses, Opportunities and Threats. The interviews/workshops had four simple questions:

1) What do you see as the main Strengths of ISMS?
2) What do you see as the main Weaknesses of ISMS?
3) What do you think are the main Opportunities for ISMS?
4) What do you think are the main Threats to ISMS?

During the sessions, the rationale of the study was presented, and the sessions were moderated (by one of the authors) maintaining neutrality to limit bias. The information was collected from all sessions

and merged into a coherent list of Strengths, Weakness, Opportunities and Threats by the authors (see section 4 for details).

The next step was to validate the findings. For this, an online survey was conducted which presented the compiled list of identified Strengths, Weakness, Opportunities and Threats and asked participants to express their views on a Likert-type scale of 1 to 5 (1: strongly disagree to 5: strongly agree). The survey also gave participants the opportunity to add new items to each of the four lists. The survey was completed by 70 participants, from various countries. To recruit survey participants a cluster sampling approach with snowballing was followed. Participants in the target groups (auditors, consultants and researchers) were identified from published literature and professional networks. The breakdown of participants and results from the survey are discussed in section 4.

3 LITERATURE REVIEW

ISO 27001 originated from a code of good practice which was publicised by the UK department of Trade and industry in 1989 and transformed further as mentioned previously. It is an internationally accepted standard that aligns information security to management systems (Anttila et al., 2012). According to Tsohou et al. (2010) and Humphreys (2008) the security controls that are implemented in the standard are customized to different organizational needs; they went further to define the standard as flexible as it can fit into any type of organization and cuts across different sectors of the economy. Brenner (2007) states that the standard is seen as a comprehensive program that incorporates risk and security management, IT governance and compliance. It also ensures that the right and appropriate resources (people, processes and technologies) are put together to enhance the management of security and risk. Susanto12 et al. (2011) compared the ISO 27001 standard with selected other standards and concluded that in the information security world it is widely used. However, Barlette and Fomin (2008) are of the opinion that the global adoption of the standard is low in comparison with quality management and environmental management systems standards. Saint-

Germain (2005) defined ISO 27001 certification as a public declaration that provides evidence of an organization's potential to manage and implement information security. However, for SMEs the expense of adoption and certification of the standard can be a barrier to them embracing it (Barlette and Fomin, 2008). Valdevit and Mayer (2010) in their study concluded that SMEs have the intention to be certified but do not have the required tools to commence. To address the issue of certification cost for SMEs Fenz et al. (2007) proposed an ontological mapping of the standard to improve the level of automation surrounded by the certification process in order to reduce the required cost and time. Susanto et al. (2011) argues that the difficulty of implementation can be a result of inadequate document preparation and other related strategies for information security. Brewer and Nash (2005) agreed with the argument of the difficulty in implementation and related it to the high financial cost and time consumption.

This clearly highlights that the standard is not perfect and provides ample opportunity for improvements. Of course, ISO 27001 is not unique in this respect; Existing literature investigates general information security and information technology framework evaluation as well as evaluation of ISO 27001 in particular.

In their work on Information Security Management Evaluation Systems Jo et al. (2011) discuss a range of existing Information Security Management Systems (ISMS) and present a comparative analysis addressing issues within these systems. Instead of offering direct improvement suggestions for individual ISMS the paper proposes an information security management evaluation system (ISMES) allowing implementer and maintainer to identify weaknesses for further improvements. However, this approach is more geared towards implementer of ISMS within organisations and governments rather than to support maintainers of the actual framework in their improvement efforts.

Shojaie et al. (2014) analyse differences within the ISO 27001 standard based on changes in the Annex A between the 2005 and 2013 revision. The authors argue that classifying the controls to known categories presents a suitable guide for evaluating the performance and efficiency of the updated

standard. They highlight changes in the control categories and, based on information security breach surveys, draw conclusions on improvement effectiveness by category achieved through these changes. They conclude that for ISO 27001:2013 their control category 'data' shows the greatest level of improvement but for 'people' and 'network' categories additional security controls are likely needed.

The work of Reza et al. (2013) also makes the point on framework improvement requirements on the people, or human, factor. In their paper the researchers identify direct and indirect human factors with impact on information security management systems and illustrate that these factors are main causes for the security incidents. They conduct a case study based SWOT analysis mapping responses to the SWOT factors with the goal to provide a model for improvement of the role of the human in ISMS. They highlight the need to further improve ISMS in this respect but also concede that it is difficult to fit human behaviour in ISMS models.

McNaughton et al. (2010) investigate the IT Infrastructure Library (ITIL) in respect to IT Service Management (ITSM) with the goal to design a holistic evaluation framework for ITIL improvements. The paper describes a design research approach combined with a contextual inquiry of industry experts to assess the framework. The contextual inquiry guided experts to focus on areas relevant to ITSM, ITIL best practice, quality attributes of the framework, and modifications and directions needed. The paper finds that their framework provides a good step towards developing an improved holistic evaluation approach for ITSM although they consider their work as only partially validated and recommend further proof of concept testing.

4 SWOT WORKSHOP ANALYSIS RESULTS

SWOT analysis is a technique that originated from Albert Humphrey in the 1960s and 1970s as a leader in a research project. It is a strategic planning tool that is used to assess strengths, weaknesses, opportunities and threats which are present in an enterprise or in a given condition in an organization

that requires decision making in pursuing an objective (Wang, 2007). Houben et al. (1999) see SWOT analysis as a flexible instrument suitable for managers of SMEs to gain insights into relevant aspect of the organization and take actions where necessary. This study conducted a SWOT analysis on the ISO 27001 standard to identify ways it can be enhanced. Based on the interviews conducted, we categorized the elements of the SWOT analysis into strengths, weaknesses, opportunities and threats as follows.

4.1 Strengths

Karppi et al. (2001) defined 'Strengths' as a tool or resource that an enterprise can use in achieving its objectives effectively. Mintzberg (2003) went further to relate strengths to competitive advantage and note-worthy competencies that an organization can benefit from. The strengths that were identified as part of the SWOT analysis are shown in Table 1 below.

Strength	*Summary*	*Details*
S1	Internationally recognised and validated	ISO27001 is internationally recognised and verified, while being validated by thousands of security professionals and participating countries (and their respective safety standards councils)
S2	Security investment planning tool	It can be used as a planning tool so that the security budget is allocated to the most relevant measure
S3	Scalability	It can be scaled to fit small or large organizations with one or multiple sites
S4	Flexibility	The Control Point based approach makes the standard flexible. Only the control points that fit the organization need to be selected and audited

S5	Compliance	It makes it straightforward to check whether an ISMS complies with standards
S6	Forces a thorough consideration of risk management	It provides much more detailed insight into Risk Management which is at the core of the standard. This is being done by leveraging on the ISO 31000 Risk Management Framework body of knowledge on Risk Management (Risk Assessment and Risk Treatment)
S7	Top-down approach	A new focus on Leadership to drive the implementation of the standard by senior management. This improves governance and accountability
S8	Clarity	The control objectives are very detailed with good checklist
S9	Performance management	The inclusion of performance management to assess the standard impact and improve on it
S10	Balance	Good balance between management systems and integrated control framework
S11	Business & Marketing tool	There is good marketing and communication around ISO 27001 (gives organisations yet another certificate to present to potential clients). It also helps build customer/client confidence and gives access to wider business opportunities (e.g. when it is a pre-requisite for tendering)
S12	Enables interoperability	Allows certified organisations to be able to exchange and manage shared data (e.g. within the Cloud) with some degree of confidence

S13	Enhances security	Improved security compared to loosely implemented baseline security

Table 1 - Overview of identified strengths

4.2 Weaknesses

Karppi et al. (2001) and Mintzberg (2003) agreed that weaknesses are limitations that can hinder an organization from reaching its goals. The weaknesses that were identified as part of the SWOT analysis are shown in Table 2 below.

Weakness	*Summary*	*Details*
W1	Adoption cost and effort	The adoption, certification and recertification costs and efforts (e.g. man hours needed to produce the documentation, etc.) can raise issues and cause hesitance when it comes to adoption by senior management
W2	Some ambiguity around Communication	There is a new clause in the standard [Communication] that is not explicit and can give room for misunderstanding between auditors and implementation consultants.
W3	Culture impact	The potential impact on organizational culture (depending on how the organisation embraces the standard)
W4	Effectiveness	It does not ensure the effectiveness of measures implemented but only their existence
W5	Misinformation	A lot of misinformation about the standard's complexity

W6	Removal of controls in the new version of the standard	Some controls were removed in the latest version of the standard such as the prompt identification of security events or incidents
W7	General misconception that the standard relates to the IT department only	Many organizations would only want to get their IT departments ISO27001 certified which would leave a high risk gap with other parts of the business.
W8	Different emphasis by different certification bodies	There is difference in emphasis by different certification bodies, where for example some focus more on context while others more on risk management
W9	Basing assessment time allocation on number of employees	As IT is a huge leverage tool, there should be less correlation between number of staff and ISMS complexity
W10	Subjectivity of awareness	Awareness could have different meaning for a 10 person small business compared to a large enterprise, for example
W11	Difficulty to understand	Small companies tend to find the control objectives difficult to understand
W12	The standard does not stipulate how detailed risk assessment should be	This could affect the way it is implemented by different companies (e.g. small businesses).
W13	Transition challenges	The transition plan can be seen as a threat to the business

Table 2 - Overview of identified weaknesses

4.3 OPPORTUNITIES

Gable and Smyth (2006) described opportunities as a representation of environmental influence that can be exploited to benefit the organization. The opportunities that were identified as part of the SWOT analysis are shown in Table 3 below.

Opportunity	*Summary*	*Details*
O1	Potential for expansion of the standard	The current standard can be potentially expanded considering the fact that information transcends technology
O2	Ease of integration with other standards	The structure of the new standard takes into cognizance the new ISO structure that enables the integration of two or more standards resulting in a seamless implementation of these standards using the same implementation effort. Additionally, it can easily be integrated into an existing management system (e.g. ISO20000, ISO22301 etc.) in an organization. With proper implementation, it can also assist with other compliance/conformity efforts
O3	Wider adoption	Other schemes, such as Cloud Security, rely on the standard so there is opportunity for wider adoption
O4	Standardizing security practices has the potential to reduce cost and increase revenue	It helps improving relationship with trading partners, shareholders and consumers which contributes to revenue, growth and the bottom line. The more international businesses adopt the approach, the fewer risks and potential liabilities (and insurance

		costs associated with information handling) we would have
O5	Lean management practices	The standard can be used to implement lean management given it can be applied to any kind of information (physical assets, data protection, intellectual property, etc.)
O6	Future proof	With up to 138 controls, it is able to address several security issues in the current environment as well as emerging ones

Table 3 - Overview of identified opportunities

4.4 THREATS

Threats are environmental factors that have the potential to destroy an organization, so it should be considered when planning strategic actions (Gable and Smyth, 2006). The threats that were identified as part of the SWOT analysis are shown in Table 4 below.

Threats	*Summary*	*Details*
T1	Minimum acceptable level of controls varies among registrars	This is despite a solid auditable standard and a standard operating procedure to guide ISO 27001 auditors
T2	Conflict of interest	Registrars are allowed to play both, the role of the auditor and implementation consultant, creating a conflict of interest (Some consulting firms are also accredited organizations)

T3	Limited Experience	Limited experience of some certification bodies
T4	Misconception that compliance means 100% security	Some organisations are under the misconception that compliance to the standard would make them experience no security breaches
T5	Similar standards to ISO 27001 are being developed in several countries	In some cases, ISO 27001 is being copied and given a different label, which is already leading to confusion
T6	Fading relevance in certain areas	It is slowly becoming less recognised as the international benchmark for areas such as Privacy and Data Protection
T7	Diminishing value	Erosion of value caused by competing organizations in some places
T8	Over-regulation issue	Risk of over-regulation by introducing too many regulations calling for the same thing (e.g. HIPAA, Data Protection, PIPEDA, PIPA, FOIPPA, etc.)
T9	Skewed incentives	More and more businesses look at certification as a marketing tool only
T10	Increased competition from other standards	Examples are the ones driven by individual countries (e.g. UK's CESG standard), which are seen by some organizations as easier to implement and address most of what ISO 27001 addresses

Table 4 - Overview of identified threats

5 SURVEY ANALYSIS

The next stage in this work was to validate the results from the SWOT analysis. For this, a survey was conducted targeting auditors, implementation consultants and researchers in the information security industry with experience in the ISO 27001 standard. The survey presented the results of the SWOT interview analysis and asked participants for their opinion on every statement using a Likert scale (1 to 5). Utilising the survey approach, we aim to validate our findings by benchmarking the extent the wider community agreed with the findings form the SWOT analysis.

We had a total number of 70 participants with 30 being auditors, 22 implementation consultants and the remaining 18 were researchers. As illustrated in Figure 1, auditors accounted for 43% of the participants, followed by implementation consultants representing 31% of the sample population, while researchers represented 26%. The confidence level and margin of error are discussed in the next section, with the survey results presented in the following section.

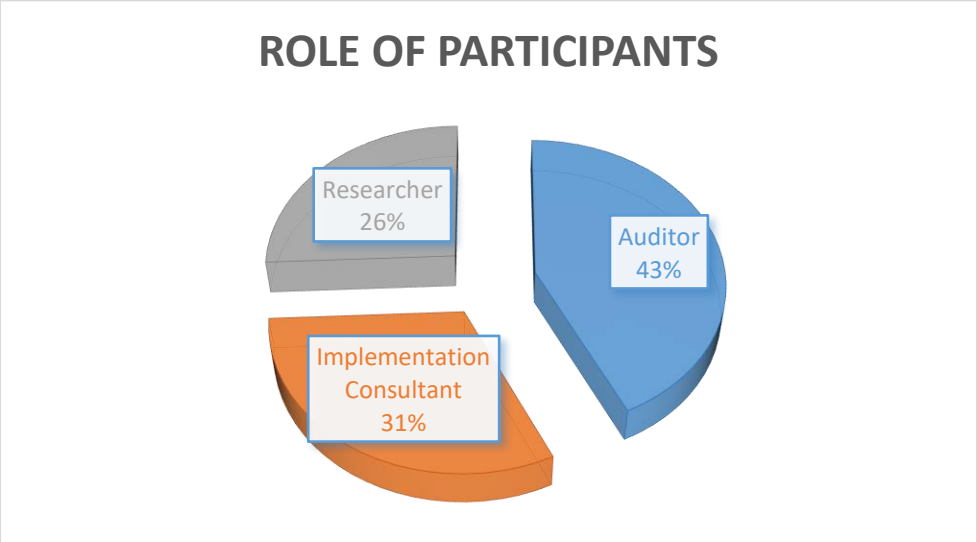

Figure 1 Representation of participants

5.1 Confidence level and margin of error

The confidence level expresses the amount of uncertainty which is tolerable in a survey. We set the desired confidence level for this study at 90% with a margin of error of 10%. As we do not know the population size we assume a relevant population size of 20,000 following normal practices for this kind of calculation (Penwarden, 2014). The resulting sample size required to match our confidence level is 68 whereas our sample size for this study is 70 which is deemed thus sufficient. The resulting expected margin of error is 9.81% which is also within our requirements.

5.2 Full group analysis by category

This section provides a high-level overview of the four categories. We analyse the survey responses with the help of diverging stacked bar charts, as well as calculate Van Der Eijk (2001) 'agreement A' and Tastle and Wierman (2007) 'Consensus' scores. Both measurements are designed to analyse ordinal data in Likert type scales, which provides an additional viewpoint on the data. Van der Eijk's measurement ranges from -1 (Disagreement) to 1 (Agreement). It represents a weighted average of the degree of agreement that exists in the simple component parts with frequency distribution considered. It does not suffer from inconsistencies of more conventional measures (Krymkowski et al., 2009). Tastle and Wierman's score is a probability distribution over a discrete set of choices with ordinal values. It's value ranges from 0 for complete disagreement, to 1 for complete agreement.

5.2.1 Strengths

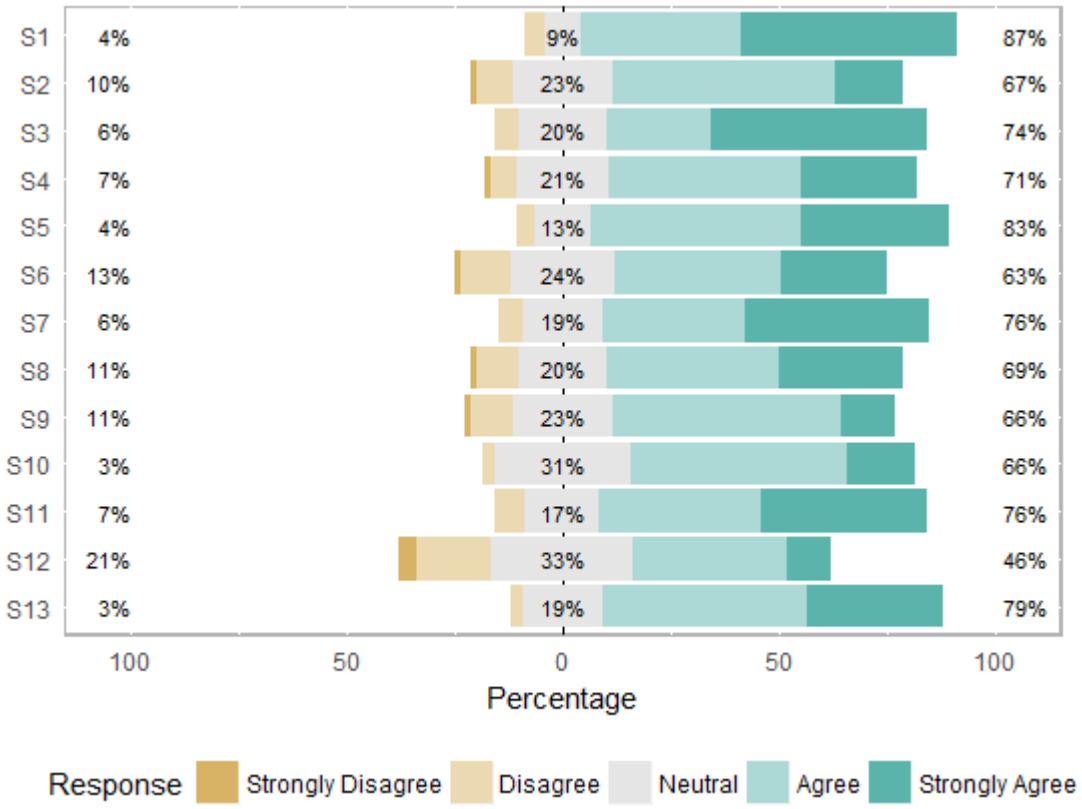

Figure 2 – Survey response distribution on Strengths

As indicated by Figure 2 we observe S1 (Internationally recognised and validated) has the highest agreement in the category 'Strengths', followed closely by S5 (Compliance) with 83%. We also note high agreement on S13 (Enhances Security) representing the practical side of ISO 27001. On the other end, we see S12 (Enables interoperability) standing out; with a 21% disagreement and 33% neutral responses it is one of the weaker 'strengths'. Implementers should consider the implications of this carefully to ensure foreseeable challenges in this space are addressed ahead of time. A further noteworthy result is the positive response on the point of ISO 27001 being a 'Business & Marketing tool' (S11). Practitioners have been arguing that information security is increasingly a competitive advantage. Our survey results support this argument as evidenced by the high agreement on this point. In addition to the basic visual response analysis, Figure 3 shows the resulting plot for the calculated TW and vdE agreement scores. We see our previous assessment confirmed, but note that

results for S11 are not as clear as assumed. While it still has good agreement scores (TW 0.691, vdE 0.535), we now see it in the middle of the field. This indicates that the participants' view on this strength are more diverse as the previous chart (Figure 2) suggests. Instead, we now notice S10 (Balance) to be one of the strengths that participants have a harmonised view on.

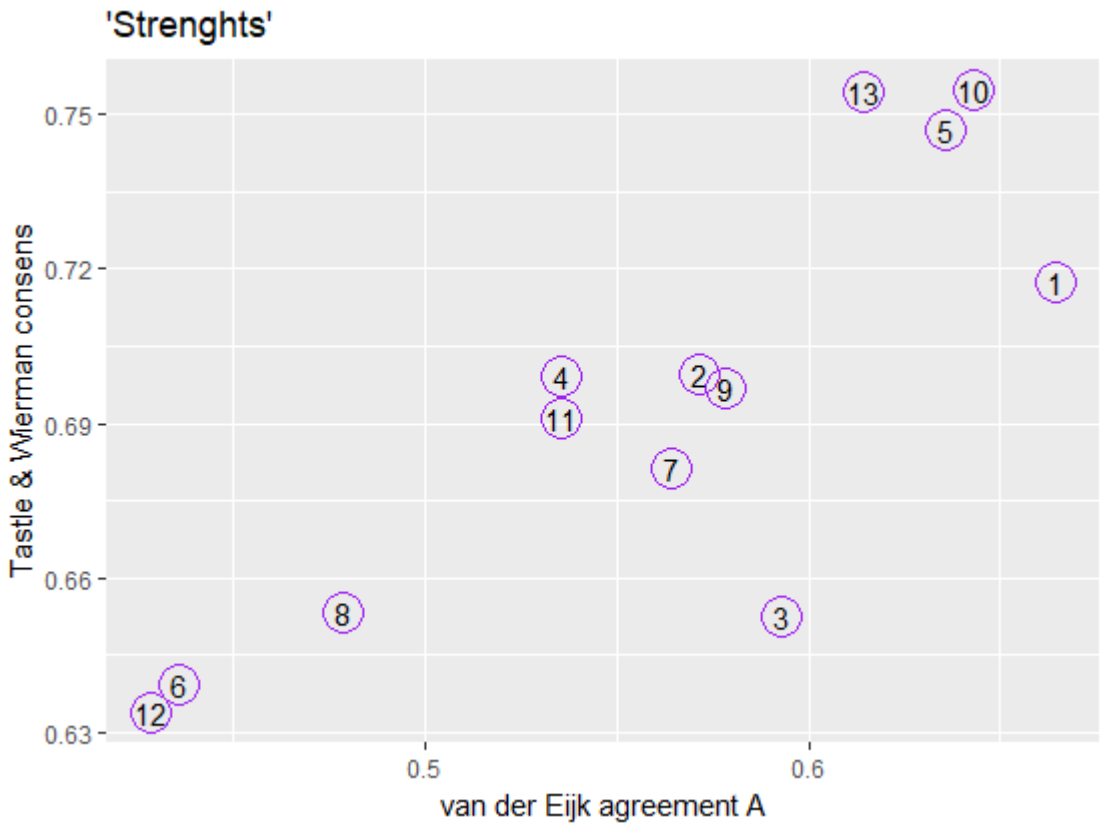

Figure 3 - Tastle & Wierman - van der Eijk agreement plot 'Strengths'

Overall, we observe agreement that the standard reached a satisfying level of international recognition which is driven by its balanced approach, its ability to scale and fulfil compliance requirements. Although, it could be argued that the creation of the standard was fundamental to spawn said compliance requirements in the first place. We conclude that there is a general acceptance of the 'Strengths' identified as part of the SWOT analysis.

5.2.2 Weaknesses

Based on the survey responses shown in Figure 4, W7 (General misconception that the standard relates to the IT department only) has the highest positive feedback in the 'Weaknesses' category.

This is followed by W8 (Different emphasis by different certification bodies) and W12 (The standard does not stipulate how detailed risk assessment should be), of which both rank 9% points lower on the agreement side. W13 (Transition challenges) and W6 (Removal of controls in the new version of the standard) are trailing the list of weaknesses and indicate a level of disagreement on the topic. If we switch the focus to the agreement analysis (Figure 5), we note that participants agree in their views on weaknesses W2, W3 and W8, but are incongruous on W10 and W13.

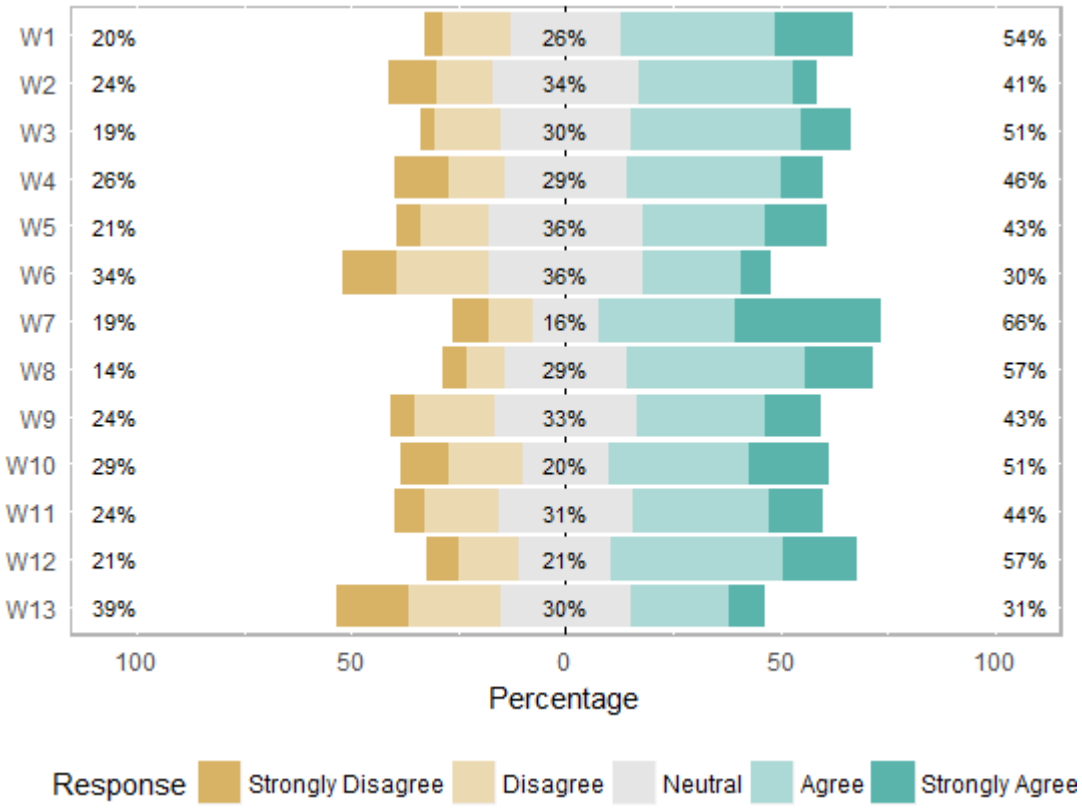

Figure 4 - Survey response distribution on Weaknesses

Based on these results it appears that ambiguity on various levels is a challenge; in this context we highlight W7, W2 and W3. These weaknesses are related to socio-technical aspects within the organisation and must rank high on the list of challenges to address for any implementer. In addition, we call out W8 describing issues with standard requirements being perceived to be not sufficiently aligned across accrediting bodies. This has serious impact on the perception of the standards' value and must be addressed by the owner of the standard. On the other hand, as evidenced by the low

agreement ratings on W13, the transition between standard revisions is not seen as a strong weakness. This should encourage the standard owners to address identified issues and introduce improvements to the standard on a more regular basis, to ensure it remains relevant to organisations.

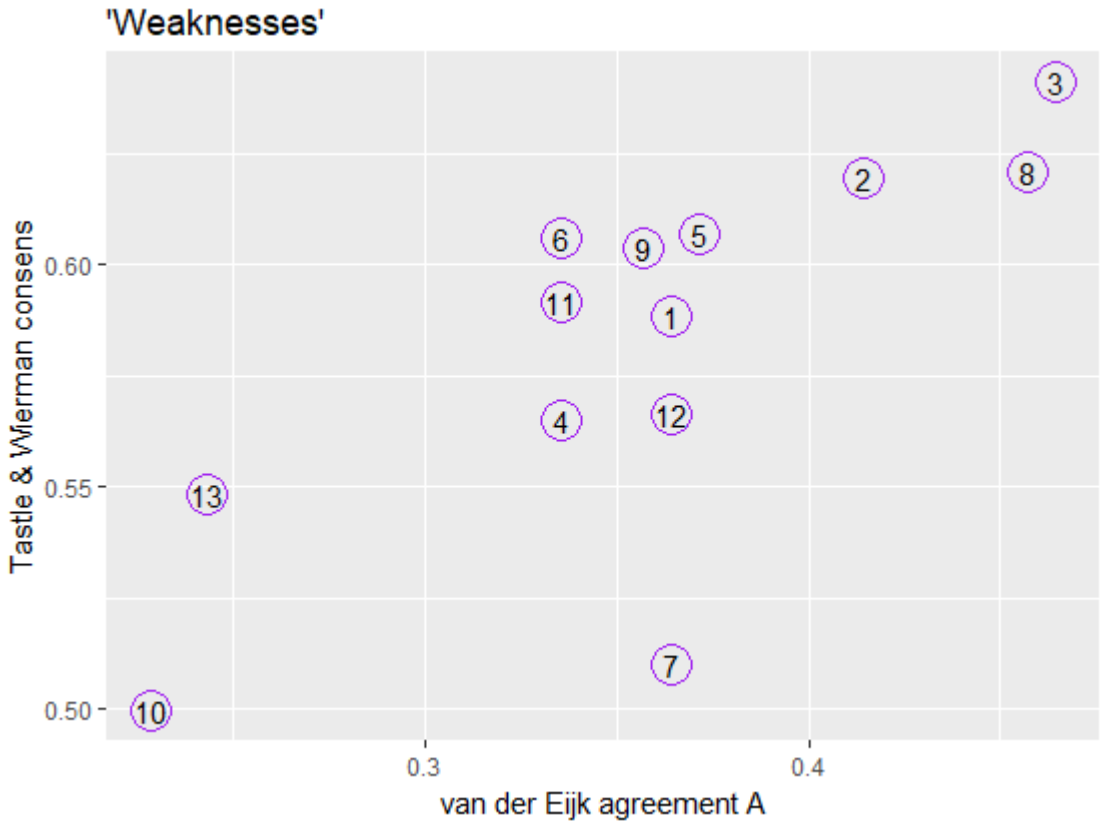

Figure 5 - Tastle & Wierman - van der Eijk agreement plot 'Weaknesses'

5.2.3 Opportunities

The Opportunities category stands out due to the generally positive stance the participant feedback takes. Across the six identified opportunities we find clear agreement that these are indeed valid opportunities for the standard. We note O2 (Ease of integration with other standards) to have the highest agreement, followed by O3 (Wider adoption) and O1 (Potential for expansion of the standard). The theme is clear; opportunities lie at the intersection of growth along wider organisational standardisation and cooperation with aligned or complementary standards.

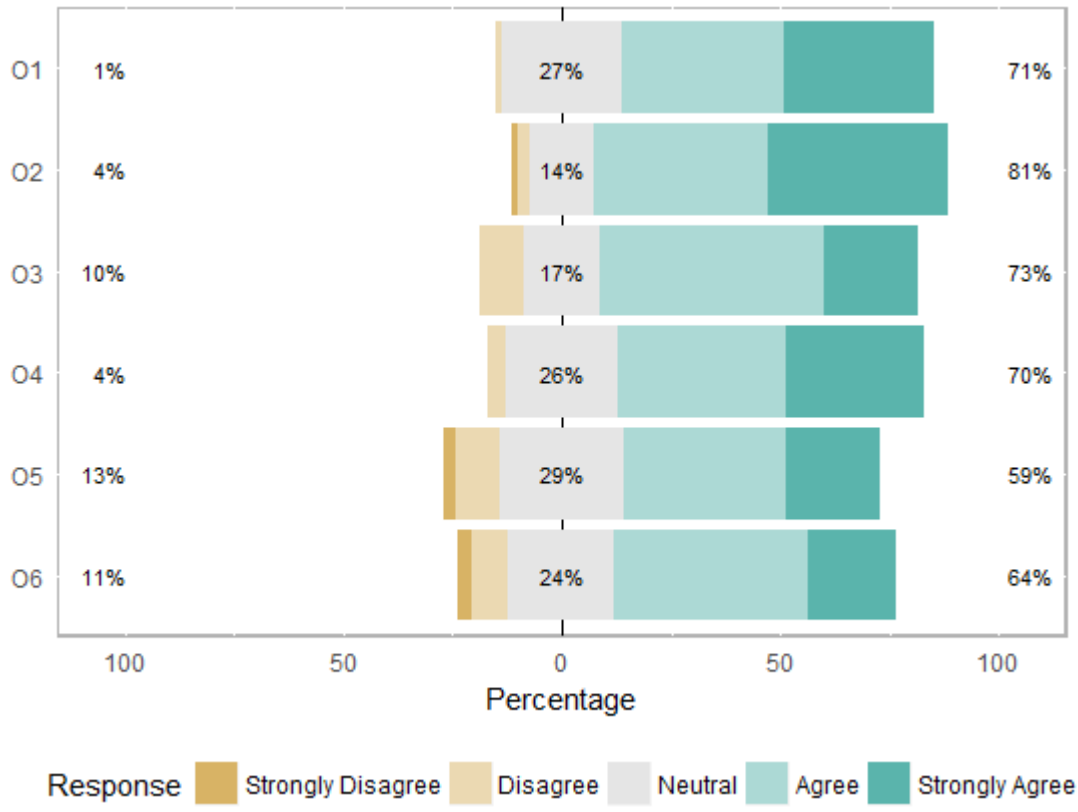

Figure 6 - Survey response distribution on Opportunities

We observe mixed, and somewhat less enthusiastic, views on O6 (Future proof) and O5 (Lean management practices). Although views are positive with solid agreement scores, the responses indicate underlying concerns. Based on context, we assume that these concerns reflect the weaknesses we've identified previously (W1, W8). It is also noteworthy that survey respondents see O1 (Potential for expansion of the standard) as a key opportunity, which complements the identified weakness W7 (General misconception that the standard relates to the IT department only).

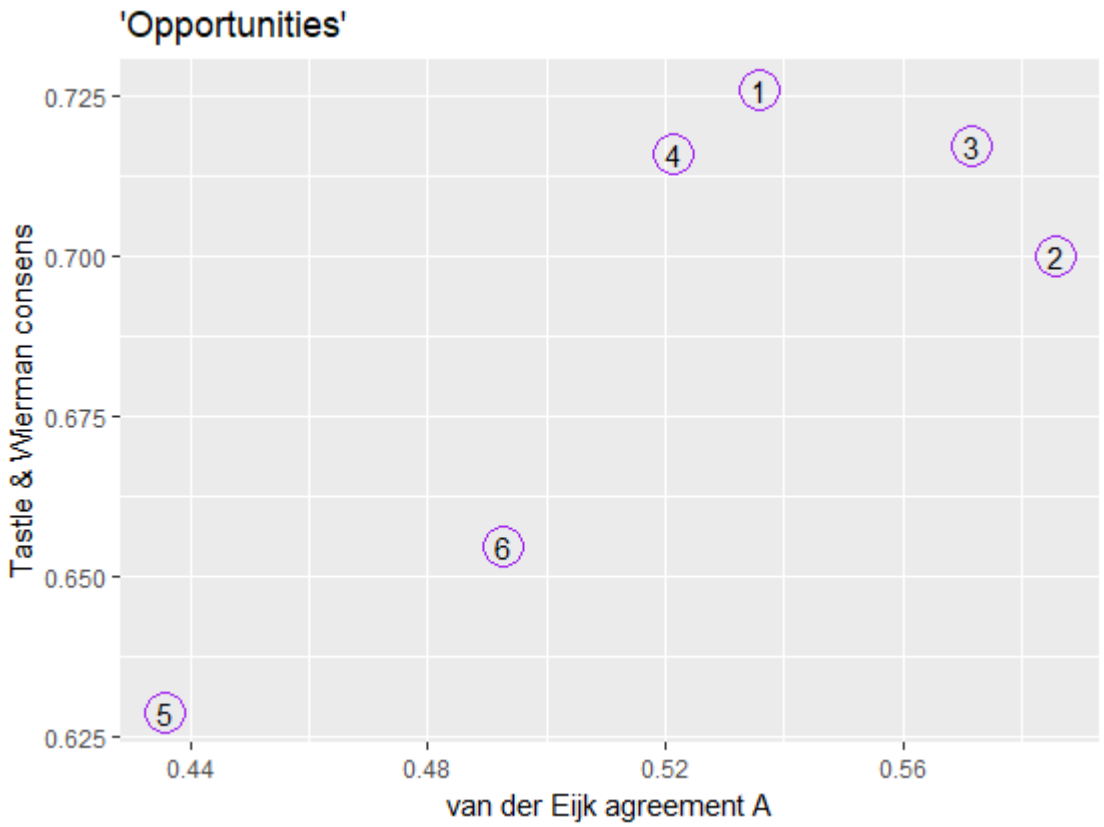

Figure 7 - Tastle & Wierman - van der Eijk agreement plot 'Opportunities'

5.2.4 Threats

Survey responses in the category ‘Threats’ were fairly distributed as Figure 8 illustrates. We immediately note T4 (Misconception that compliance means 100% security) and T9 (Skewed incentives) to stand out due to high participant agreements. This is supported by the respective TW and vdE scores (Figure 9) positioning both threats in the upper right quadrant. On the other end, we observe scores for T5 (Similar standards to ISO 27001 are being developed in several countries), T2 (Conflict of interest) and T8 (Over-regulation issue), which border on ‘no agreement’. Considering this, the best approach for stakeholders is to focus on threats T4, T7, T9 and T3. We propose that T3, T4 and T9 is highly relevant to consider for organisations pursuing certification, whereas T3, T7 and T9 must be a priority for the standard owner to keep the value proposition of the certification attractive.

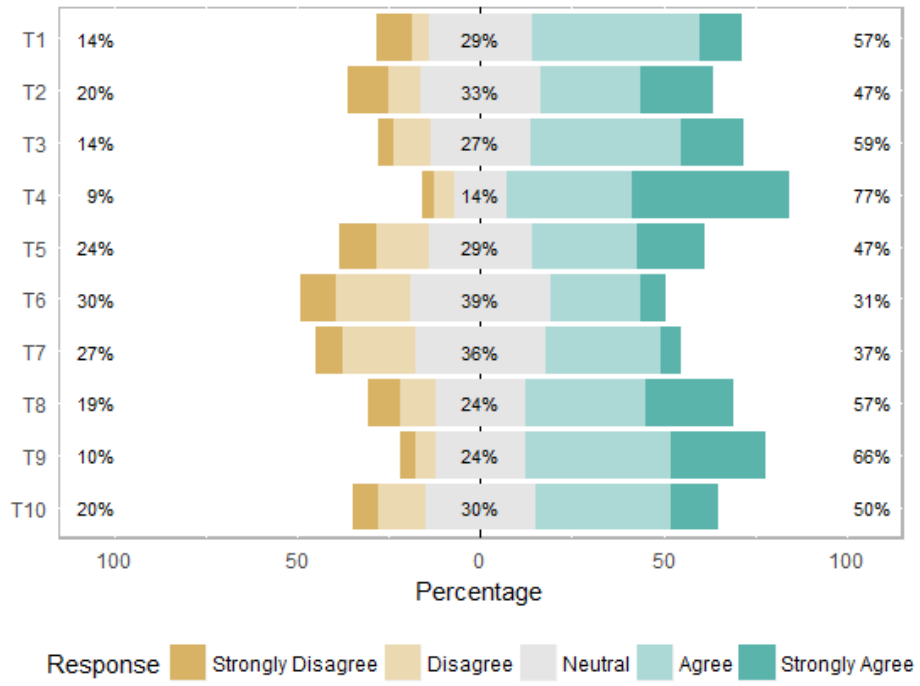

Figure 8 - Representation of positive ranking of questions in Threats

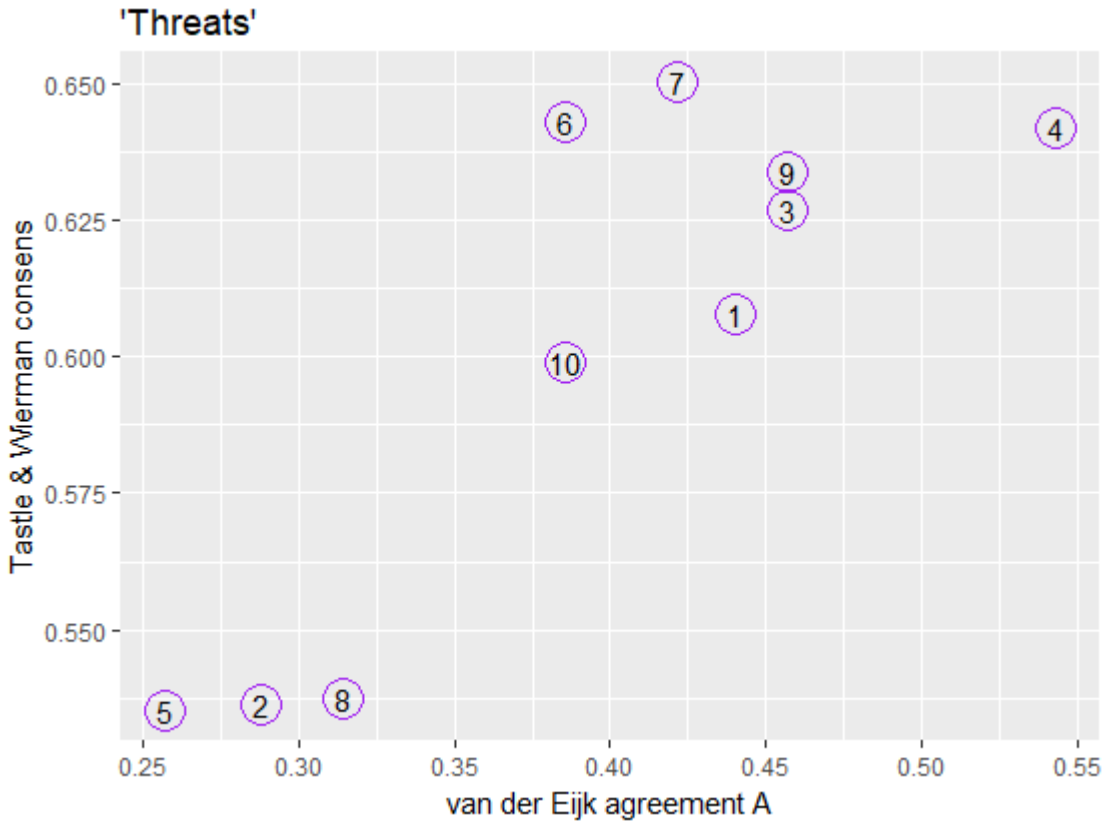

Figure 9 - Tastle & Wierman - van der Eijk agreement plot 'Threats'

5.3 Group based analysis by category

In this section, we take a look at the survey responses of each group. This provides a quick way to assess how participants viewed the Strengths, Weaknesses, Opportunities and Threats as outlined in the previous section, based on their professional role.

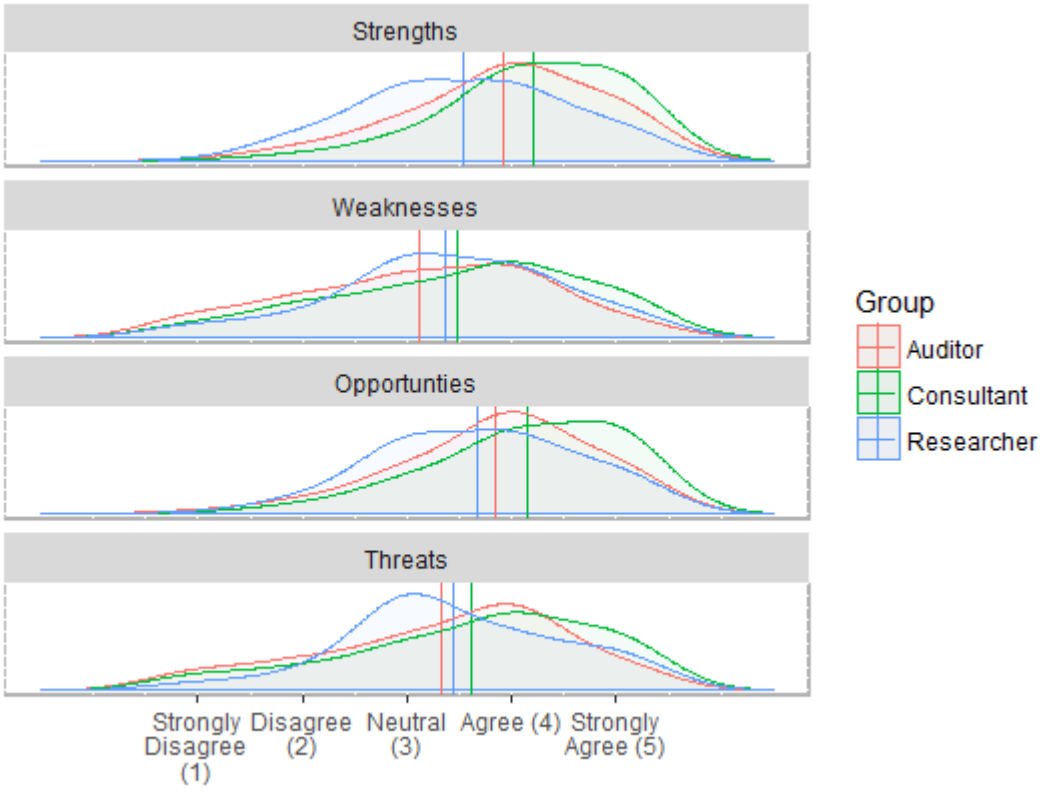

Figure 10 – Group response distribution by category

Observing the group responses for 'Strengths' we note that the implementation consultant group expresses overall stronger agreement in this category than the other groups. While auditors also show a peak on 'Agree', we see researchers taking a neutral to positive position on the strengths of the standard. From a researcher group perspective, this position is held with 'Weaknesses' as well. Again, we see consultants to have the highest level of agreement with the identified weaknesses. Auditors

show the lowest level of agreement with weaknesses, or in other words – this group is the most positive towards the standard. Overall, we see a tendency to a neutral position on the topic of weaknesses.

Responses on the topic of 'Opportunities' are comparable to those in the 'Strengths' category with a visible edge towards agreement. Again, we see the consultants group taking the most positive stance on this topic. Researchers appear slightly more agreeable with the identified opportunities than previously seen in the 'Strengths' category. We interpret this as a statement that researchers see the standard standing on a good basis but that it must improve further. The researcher group has a less defined view on the topic of 'Threats' and stands out through peaked neutral views. However, all groups show a tendency to agree with the identified threats to the standards as shown in Figure 10.

Based on the descriptive analysis above, we observed that our implementation consultants group showed a generally higher level of agreement with the four categories in the survey, whereas the researcher group tends to neutrality on the topics. In summary, we find that our subject matter experts express agreement with the identified points in each category overall.

6 RESULT VERIFICATION AND DISCUSSION

Based on the data analysis and validation so far, it is evident that the participants of the study agree with the research questions. The first research question of this study looked at the 'Strengths' and 'Weaknesses' of the ISO 27001 standard. To recapitulate, we conducted interviews with certified accreditors to get their expert views on the topic, which was then validated by researchers, auditors and implementation consultants through a survey instrument. We found that implementation consultants showed general agreement in their responses, while researchers provided mainly neutral responses. Auditors showed a balanced view on 'Strengths' with a tendency to disagree on points adverse to the standard (Weaknesses).

The second research question of the study looked at the 'Opportunities' and 'Threats' of the standard. We found that auditors and implementation consultants have a more positive tendency in their responses regarding the 'Opportunities' of the standard. Similarly to 'Weaknesses', auditors tend to show stronger disagreement than the other groups on topics critical of the standard.

In general, we found that responses to 'Strengths' and 'Opportunities' had a stronger affirmative tendency than those dealing with the 'Weaknesses' and 'Threats'. We will verify these findings statistically in the remainder of this section.

6.1 Analysis of variance (ANOVA)

ANOVA is a statistical technique and is used to determine existence of significant differences among the means of multiple sample observations. It is useful when the difference among the results cannot be presented quantitatively (Chen, 1988).

In this study, we use ANOVA to verify our findings generally. We apply statistical analysis to each group (Strengths, Weaknesses, Opportunities, Threats) assuming a null hypothesis (H_0) of no difference in opinion between participant groups. Consequently, we follow -

$$\textit{If } f_{stat} > f_{crit}\textit{, reject null hypothesis}$$

$$\textit{If } f_{stat} < f_{crit}\textit{, do not reject null hypothesis}$$

We find that all groups except 'Threats' show statistically highly significant results when compared to the corresponding f_{crit} factor. For details, please refer to Appendix A. To further investigate significant variations, we conduct a pairwise comparison utilizing parametric and non-parametric tests.

6.2 Parametric and non-parametric significance testing

To verify and better understand our survey results we decided to utilise additional statistical methods. In first instance, we used the Student's t-test approach; a t-test can be used to determine if two results show a statistically significant difference from each other. In this study, we used the t-test to check if the null hypothesis should be rejected assuming the p-value shows a significance level of at least 0.05.

In this case, our null hypothesis (H_0) is that the opinion of two different groups (e.g. Auditors vs Consultants) is the same regarding the results of the SWOT analysis. Our calculations are based on a two-tailed test with independent sample distribution assuming unequal variances. As our normality assumptions for some of the group data does not hold, as verified through Shapiro-Wilk testing, we verified significance through non-parametric testing (Mann-Whitney Test for Two Independent Samples).

6.2.1 Interpretation for strengths

	Auditor	Consultant	Researcher
Auditor		0.027042675	0.015996650
Consultant	0.049611368		0.000021075
Researcher	0.005450755	0.000031893	

Table 5 - Parametric and non-parametric p-values 'Strength'

To understand differences between groups in the 'Strength' category, we compared each group responses with the responses of the other groups. Table 5 provides an overview of the p-values between groups where the results in the upper triangle show the results of parametric tests and the lower triangle shows results of the corresponding non-parametric tests. We observe statistically significant differences between each groups' responses. Based on the data we conclude that strengths of ISO 27001 are viewed similarly between Auditors and Consultants as we merely approached statistical significance in the non-parametric test (p .05). However, we note a statistically highly significant difference in perception of strengths of the standard between Researchers and both other groups. This is particularly strong between our researchers and consultants (non-parametric p 0.00003).

6.2.2 Interpretation for weaknesses

	Auditor	Consultant	Researcher
Auditor		0.088779791	0.117366447
Consultant	0.145959329		0.543016100
Researcher	0.616755925	0.270875908	

Table 6 - Parametric and non-parametric p-values 'Weakness'

Repeating our statistical analysis of the survey results we found that there is no statistically significant difference in how our survey groups viewed 'Weaknesses' of the standard; thus, we cannot reject H_0 in regard to 'Weaknesses'. It is worth noting that statistical dispersion for our researcher group is considerably lower, as measured by sample variance (0.12) and average absolute deviation (AAD, 0.3), than for the other two groups. This leads us to believe that while researcher do not perceive the weaknesses of the standard drastically different than practitioners, they are more aligned in their understanding of the weaknesses. This could present an opportunity for researchers to provide assistance to practitioners helping them to focus their understanding of weaknesses in the standard. The assumption is that based on a better understanding of the weaknesses (or at least a better aligned understanding) between groups future improvements in the standard can be achieved more easily.

6.2.3 Interpretation for opportunities

	Auditor	Consultant	Researcher
Auditor		0.046885986	0.136695603
Consultant	0.043501282		0.000760290

Researcher	0.088442599	0.002435198	

Table 7 - Parametric and non-parametric p-values 'Opportunities'

Views on the 'Opportunities' of the standard are varying between the groups. We did not observe a statistically significant deviation between the auditor and researcher groups; however, we note a significance (parametric p 0.002, non-parametric p 0.0007) in response variation between researchers and consultants. Based on the survey results it appears there is a considerable difference in viewpoint regarding the standards' positive attributes ('Strength', 'Opportunity') between researchers and consultants. We do not have sufficient information available to draw definitive conclusions but the existence of a slight cognitive bias (e.g. a form of self-serving bias) affecting the implementation consultant group appears a possibility.

6.2.4 INTERPRETATION FOR THREATS

	Auditor	Consultant	Researcher
Auditor		0.195737775	0.512579241
Consultant	0.170497997		0.378425706
Researcher	0.949059681	0.276835998	

Table 8 - Parametric and non-parametric p-values 'Threats'

Similarly to the findings on 'Weaknesses' our analysis of the survey results did not show statistically significant outcomes. We cannot reject our H_0 that there are no differences in the opinions between the groups regarding 'Threats' to the standard.

6.3 Keeping the standard on its TOWS

To round out the discussion on our findings, we are offering a view on how the identified strengths, weaknesses, opportunities and threats can be utilised to improve the standard. We present a TOWS

matrix (Table 5) to show how the strengths and opportunities of the standard can be used to address the weaknesses and threats. The TOWS matrix is a situational analysis tool used by managers for strategy development, plan and actions for executing effectively on the objectives and mission of an organization. The strategies include SO strategy (Maxi-Maxi), WO strategy (Mini-Maxi), ST strategy (Maxi-Mini) and WT strategy (Mini-Mini) (Al-Mayahi and Mansoor, 2012). We make no claim that our proposed strategies are the only strategies or necessarily the best strategies that can be followed. They provide one perspective based on the findings in this study and are proposed in line with the insights documented in previous sections.

SO Strategy (*Maxi-Maxi*)	WO Strategy (*Mini-Maxi*)
• [S1, O1] Capitalize on the international recognition as a way to expand the standard • [S12, O3] Improve on the interoperability of the standard to give room for wider adoption	• [W1, W5, O1] Propose a lighter version of the standard to make it cheaper to adopt, simplified, less complex and dependent • [W5, O2] Use the ease of integration with other standards to reduce the complexity • [W1, W4, O4] Focus on standardizing the security practices as it has potential to reduce cost and provides confidence to clients ensuring effectiveness of implemented measures • [W6, O6] Create a balance with available controls to address security issues in the organisation

	• [W3, O5] Use the implementation of lean management to help employees embrace the standard in a positive way, giving room for confidence
ST Strategy (*Maxi-mini*)	WT Strategy (*Mini-Mini*)
• [S1, T5] Capitalize on the international recognition of the standard to reduce confusion on the development of similar standards • [S9, T4] Use performance management to check the compliance of employees and security awareness to reduce misconceptions about compliance equal security • [S11, T7, T9] Create awareness to inform organisations of the importance of certification aside being a marketing tool to avoid erosion of value • [S7, T2] Use the organisations senior management to define roles to avoid conflict of interest	

Table 9 - TOWS matrix

7 STUDY LIMITATIONS

Our research carries some limitations inherent to the survey instruments, grounded theory and SWOT analysis that must be acknowledged. The first limitation is sampling. We have limited information

about the participants in our research as many are recruited randomly from online communities (Dillman, 2000, Stanton, 1998). An additional limitation is known as the self-selection bias (Thompson et al., 2003)). This simply means that not every contact that received an invite to participate in our survey responds to it. This self-selection for participation can result in a bias and must be acknowledged. General survey mechanics provided further challenges; low response rate issues resulted in restricted confidence levels and lower margin of error. This is a common limitation of surveys aimed at field experts rather than the general populous (Penwarden, 2014). Access issues can also be seen as a limitation of this study. Our approach was to post participation invitations in professional online communities as well as requesting participation through targeted emails. Some members of the online communities my find this behaviour rude (Hudson and Bruckman, 2004) or consider it Spam (Andrews et al., 2003).

8 SUMMARY AND FUTURE WORK

The implementation of information security management standards come with benefits as evidenced by the 'Strengths' listed in this research. But implementation of such an ISMS can be challenging especially for small and medium size organizations (SME) due to a variety of reasons, some of which are listed as 'Weaknesses' in this research. In this study we aimed to answer the following questions; 1) what are the strengths and weaknesses of the ISO 27001 standard; 2) what are the opportunities and threats of the ISO 27001 standard and 3) how can the strengths and opportunities be leveraged to address the weaknesses and threats. To this end the study focused on auditors, researchers and implementation consultants familiar with the standard to solicit their views. Qualitative and quantitative research methods were employed to answer our research questions and achieve the objectives. The qualitative research presented the findings while the quantitative approach was used to validate it. We identified key factors across all four areas (SWOT) affecting the standard with strong agreement on top factors across all participant groups.

Our findings show that there is a generally positive view on the ‘Strengths’ and ‘Opportunities’ compared to that of ’Weaknesses’ and ‘Threats’. The results show that implementation consultants take a particular positive outlook on the areas surveyed (SWOT) compared to those participants identified as researchers, who expressed mainly neutral views. We identified statistically significant differences in the perception of the ‘Strengths’ and ‘Opportunities’ across the groups but also found that there is no significant variance in the perception of ‘Threats’.

In addressing the third research question, we used a TOWS matrix to show how the strengths and opportunities of the standard can be used to address the weaknesses and threats. In the WO strategy (mini-maxi), we proposed a lighter version of the standard to make it cheaper to adopt, simplified, less complex and dependent.

While this paper addresses the SWOT analysis of the ISO 27001 standard and proposes a lighter version in order to enhance the use across SMEs, further research is proposed to conduct a case study scenario to validate our results. More research will be required to take into consideration different SMEs’ industries. The area of coverage can also be considered in further research to address the issues in relation to the geographical locations of participants.

9 REFERENCES

Al-Mayahi, I. and Mansoor, S. 'UAE E-goverment: SWOT analysis and TOWS Matrix'. *ICT and Knowledge Engineering (ICT & Knowledge Engineering), 2012 10th International Conference on*: IEEE, 201-204.

Andrews, D., Nonnecke, B. and Preece, J. (2003) 'Electronic survey methodology: A case study in reaching hard-to-involve Internet users', *International Journal of Human-Computer Interaction,* 16(2), pp. 185-210.

Anttila, J., Jussila, K., Kajava, J. and Kamaja, I. 'Integrating ISO 27001 and other managerial discipline standards with processes of management in organizations'. *Availability, Reliability and Security (ARES), 2012 Seventh International Conference on*: IEEE, 425-436.

Barlette, Y. and Fomin, V. V. 'Exploring the suitability of IS security management standards for SMEs'. *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual*: IEEE, 308-308.

Beckers, K., Heisel, M., Solhaug, B. and Stølen, K. (2014) 'ISMS-CORAS: A Structured Method for Establishing an ISO 27001 Compliant Information Security Management System', *Engineering Secure Future Internet Services and Systems*: Springer, pp. 315-344.

Brenner, J. (2007) 'ISO 27001: Risk management and compliance', *RISK MANAGEMENT-NEW YORK-,* 54(1), pp. 24.

Brewer, D. and Nash, M. (2005) 'The Similarity between ISO 9001 and BS7799-2 ', pp. 4, Available: Gamma Secure Systems Ltd. Available at: http://www.gammassl.co.uk/research/archives/ISMS/9001Similarities.pdf.

Broderick, J. S. (2006) 'ISMS, security standards and security regulations', *Information Security Technical Report,* 11(1), pp. 26-31.

Chen, C.-L. (1988) 'Analysis of variance'.

Creswell, J. W. (2013) Research design: Qualitative, quantitative, and mixed methods approaches. 4 edn.: Sage publications.

Dillman, D. A. (2000) Mail and internet surveys: The tailored design method. Wiley New York.

Fenz, S., Goluch, G., Ekelhart, A., Riedl, B. and Weippl, E. 'Information security fortification by ontological mapping of the ISO 27001 standard'. *Dependable Computing, 2007. PRDC 2007. 13th Pacific Rim International Symposium on*: IEEE, 381-388.

Gable, G. and Smyth, R. (2006) 'Administrative Placement of the Information Systems Discipline in Universities-A SWOT Analysis of Queensland University of Technology', *PACIS 2006*, pp. 1374-1388.

Hill, T. and Westbrook, R. (1997) 'SWOT analysis: It's time for a product recall', *Long Range Planning,* 30(1), pp. 46-52.

Honan, B. (2010) ISO27001 in a Windows Environment: The best practice handbook for a Microsoft® Windows® environment. IT Governance Ltd.

Houben, G., Lenie, K. and Vanhoof, K. (1999) 'A knowledge-based SWOT-analysis system as an instrument for strategic planning in small and medium sized enterprises', *Decision support systems,* 26(2), pp. 125-135.

Hudson, J. M. and Bruckman, A. (2004) '"Go away": participant objections to being studied and the ethics of chatroom research', *The Information Society,* 20(2), pp. 127-139.

Humphreys, E. (2008) 'Information security management standards: Compliance, governance and risk management', *information security technical report,* 13(4), pp. 247-255.

International Standards Organisation (2014) *ISO Survey 2014*. ISO Survey. Available at: http://www.iso.org/iso/iso-survey.

Jo, H., Kim, S. and Won, D. (2011) 'Advanced Information Security Management Evaluation System', *Ksii Transactions on Internet and Information Systems,* 5(6), pp. 1192-1213.

Johnson, R. B. and Onwuegbuzie, A. J. (2004) 'Mixed methods research: A research paradigm whose time has come', *Educational researcher,* 33(7), pp. 14-26.

Karppi, I., Kokkonen, M. and Lähteenmäki-Smith, K. (2001) 'SWOT-analysis as a basis for regional strategies', *Nordregio WP,* 4, pp. 80.

Krymkowski, D. H., Manning, R. E. and Valliere, W. A. (2009) 'Norm Crystallization: Measurement and Comparative Analysis', *Leisure Sciences,* 31(5), pp. 403-416.

McNaughton, B., Ray, P. and Lewis, L. (2010) 'Designing an evaluation framework for IT service management', *Information & Management,* 47(4), pp. 219-225.

Mintzberg, H. (2003) The strategy process: concepts, contexts, cases. Pearson Education.

Penwarden, R. (2014) *How to get the Best Data by Optimizing Your Target Sample Group*. FluidSurveys University: FluidSurveys. Available at: http://fluidsurveys.com/university/create-surveys-work-target-sample-group/ (Accessed: 2015-04-03.

Prislan, K. and Bernik, I. 'Risk management with ISO 27000 standards in information security'. *Proceedings of the 9th WSEAS international conference on Advances in e-activities, information security and privacy*: World Scientific and Engineering Academy and Society (WSEAS), 58-63.

Reza, A., Shareeful, I., Hamid, J. and Ameer, A.-N. (2013) 'Analyzing Human Factors for an Effective Information Security Management System', *International Journal of Secure Software Engineering (IJSSE),* 4(1), pp. 50-74.

Saint-Germain, R. (2005) 'Information security management best practice based on ISO 17799', *Information Management Journal,* 39(4), pp. 60-66.

Shojaie, B., Federrath, H. and Saberi, I. 'Evaluating the Effectiveness of ISO 27001: 2013 Based on Annex A'. *Availability, Reliability and Security (ARES), 2014 Ninth International Conference on*, 8-12 Sept. 2014, 259-264.

Stanton, J. M. (1998) 'An empirical assessment of data collection using the Internet', *Personnel Psychology,* 51(3), pp. 709-725.

Susanto12, H., Almunawar, M. N. and Tuan, Y. C. (2011) 'Information security management system standards: A comparative study of the big five'.

Susanto, H., Almunawar, M. N. and Tuan, Y. C. (2011) 'I-SolFramework View on ISO 27001. Information Security Management System: Refinement Integrated Solution's Six Domains', *Asian Transactions on Computers,* 1(03).

Tastle, W. J. and Wierman, M. J. (2007) 'Consensus and dissention: A measure of ordinal dispersion', *International Journal of Approximate Reasoning,* 45(3), pp. 531-545.

Thompson, L. F., Surface, E. A., Martin, D. L. and Sanders, M. G. (2003) 'From paper to pixels: Moving personnel surveys to the Web', *Personnel Psychology,* 56(1), pp. 197-227.

Tipton, H. F. and Krause, M. (2012) *Information Security Management Handbook.* 6th edn. Boca Raton: Auerbach Publications.

Tsohou, A., Kokolakis, S., Lambrinoudakis, C. and Gritzalis, S. (2010) 'A security standards' framework to facilitate best practices' awareness and conformity', *Information Management & Computer Security,* 18(5), pp. 350-365.

Valdevit, T. and Mayer, N. 'A Gap Analysis Tool for SMEs Targeting ISO 27001 Compliance'. *ICEIS (3)*, 413-416.

Van Der Eijk, C. (2001) 'Measuring Agreement in Ordered Rating Scales', *Quality and Quantity,* 35(3), pp. 325-341.

Wang, K.-c. 'A process view of SWOT analysis'. Proceedings of the 51st Annual Meeting of the ISSS-2007, Tokyo, Japan.

10 APPENDIX A

Tables E1-E4 shows the ANOVA interpretation for the SWOT of the standard

Table E.1- ANOVA interpretation for strengths of the standard

Source of Variation	SS	df	MS	F	P-value	F crit
Between Groups	3.01267	2	1.506335	15.3898	1.48E-05	3.259446
Within Groups	3.523636	36	0.097879			
Total	6.536306	38				

Table E.2- ANOVA interpretation for weaknesses of the standard

Source of Variation	SS	df	MS	F	P-value	F crit
Between Groups	0.923932	2	0.461966	4.798815	0.014206	3.259446
Within Groups	3.465602	36	0.096267			
Total	4.389534	38				

Table E.3- ANOVA interpretation for opportunities of the standard

Source of Variation	SS	df	MS	F	P-value	F crit

Between Groups	0.900599	2	0.450299	6.174382	0.011057	3.68232
Within Groups	1.093954	15	0.07293			
Total	1.994553	17				

Table E.4- ANOVA interpretation for threats of the standard

Source of Variation	SS	df	MS	F	P-value	F crit
Between Groups	0.396526	2	0.198263	1.548077	0.230947	3.354131
Within Groups	3.457903	27	0.12807			
Total	3.854429	29				