



[1]

Evaluating the effectiveness of ISO 27001 Implementation in Enhancing Organisational Cybersecurity

Deian Rhys Treharne | 2120039 | LSN Diffusion Ltd



Research Context

- Importance of organisational cybersecurity
- Cybersecurity is continuously developing
- Potential damages caused by cyberattacks

Research Proposal - Deian Rhys Treharne (2120039)

1.2 Research Problem

ISO 27001 implementation is becoming more popular through organisations worldwide. According to IT Governance, it is reported that *“67,326 organisations worldwide have ISO 27001 certification as of 31 December 2022. This continues the trend of a year-on-year increase”* [6]. However, is there sufficient evidence to support how effective the implementation of ISO 27001 really is? Due to the standard being standardised for all organisations, does the implementation process genuinely enhance their cybersecurity?

The researcher's involvement in the implementation of the ISO 27001 standard has developed the researcher's knowledge and understanding of the standard and the benefits to the organisation in achieving certification. This has initiated the researcher to undertake further research on the effectiveness of ISO 27001 implementation in enhancing organisational cybersecurity. The researcher's aim and objectives are to investigate this problem and to reach a conclusion whether ISO 27001 effectively improves organisational security.

Research Problem

3. Aim & Objectives

3.1 Aim:

The aim of this project is to evaluate the effectiveness of ISO 27001 implementation in enhancing organisational security.

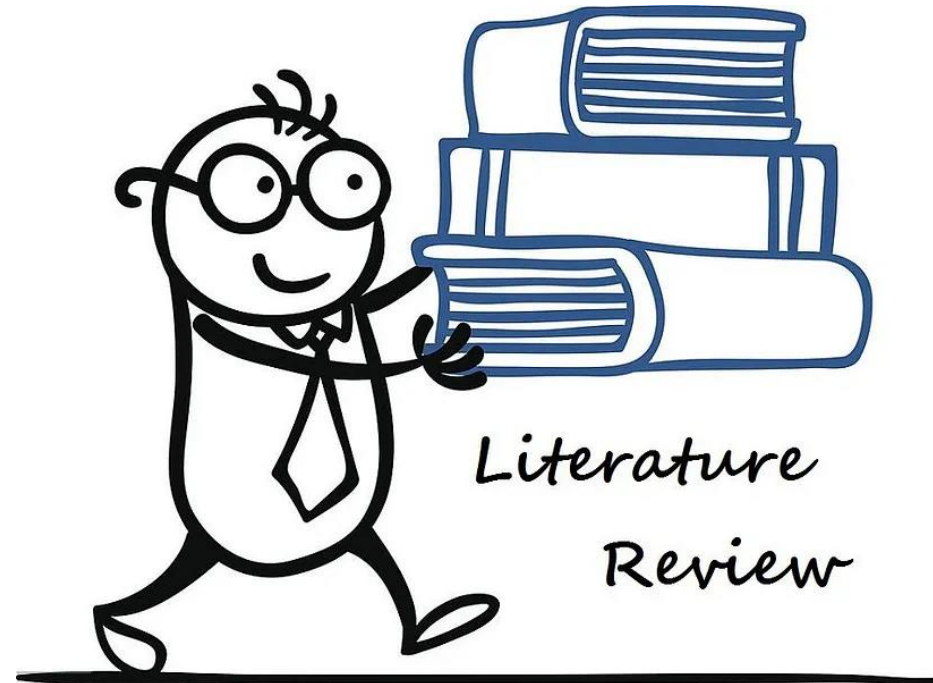
3.2 Objectives:

- Identify and review the domains within the ISO 27001 framework
- Evaluate cybersecurity measures before and after implementation of ISO 27001
- Identify barriers and possible solutions for organisations during the implementation phase of ISO 27001
- Identify barriers and possible solutions for organisations when maintaining compliance to ISO 27001 standard

Research Aims & Objectives

Literature Review – Introduction

- Context
- Purpose
- Structure



▲ 2.2 ISO 27001 Overview

The International Organisation for Standardisation known as ISO. ISO 27001 is the first standard in the ISO 27000 series. ISO 27001 was initially published in October of 2005 however it was reviewed in 2013 and 2022 due to the advancing digital technologies and associated risks [8]. The ISO 27001 is a recognised framework to support organisations with their information security management system (ISMS). The ISO 27001 framework has 14 domains, some are listed below: [9]

Information Security Policy [9]	Organisation of Information Security [9]
Human Resources Security [9]	Asset Management [9]
Access Control [9]	Cryptography [9]
Physical and Environmental Security [9]	Operations Security [9]
Systems Acquisition, Development and Maintenance [9]	Communications Security [9]
Supplier Relationships [9]	Information Security Incidents Management [9]
Information Security Aspects of Business Continuity [9]	Compliance [9]

Figure 2- ISO 27001 Framework Categories Table

Literature Review – ISO 27001 Overview

2.3 Role of ISO 27001 in Enhancing Organisational Cybersecurity

The aim of ISO 27001 is to improve the quality of security within organisations. The implementation of ISO 27001 cannot prevent the risks of a cyberattack, but it can reduce the impact of a cyberattack. For example, in July 2019 British Airways was fined £183 million for failing to prevent the phishing email that was sent out to people that used a fake website. This is evidence of the consequences associated with inadequate cybersecurity [10].

The ISO 27001 is not the only information security framework. Other standards include the National Institute of Standards and Technology (NIST) [11] and the Control Objectives for Information and Related Technologies (COBIT) [12]. The difference between ISO 27001, COBIT and NIST as follows:

COBIT: COBIT focuses on the IT Governance and management [13]

ISO 27001: ISO 27001 focuses on information security and management [13]

NIST: NIST focuses on enhancing the security and resilience of information systems [13]

Literature Review – Role of ISO 27001 in Enhancing organisational Cybersecurity

Literature Review – Effectiveness of ISO 27001 Implementation Case Study

2.4 Effectiveness of ISO 27001 Implementation Case Study

An international organisation named 'Fredrickson International' was once an organisation without ISO 27001 certification. This meant their cybersecurity environment was weak and inadequate which put all their data and assets at risk of a cyberattack which could have cost them millions. Simon Jones the Managing Director of Fredrickson International stated *"We feel as an organisation we simply cannot afford to take an ad-hoc approach to managing information security risk. With BSI's help we have implemented a system that has provided both an appropriate and affordable level of protection to our customers"* [14]. This case study suggests that implementing an ISMS provides high level of security to an organisation. Darren Shorney Head of Technical at Alcumus ISOQAR identifies 10 nonconformities with the implementation of ISO. These non-conformities could impact organisational cybersecurity after the implementation. Below is the most common nonconformities Darren Shorney identified: [15]

Research Proposal - Deian Rhys Treharne (2120039)

Lack of senior management [15]	Inadequate security controls for third-party providers [15]
Inadequate physical security [15]	Lack of regular security testing [15]
Not updating and maintaining business continuity plan [15]	Failure to conduct regular risk assessments [15]
Inadequate monitoring of privileges access [15]	Inadequate monitoring of mobile phones and laptops [15]
Failure to comply with legal and regulatory requirements [15]	Inadequate security training [15]

Figure 3 Darren Shorney's most common nonconformities table

2.5 Challenges and Barriers in Implementing ISO 27001

One of the most common challenges when implementing an ISO 27001 is a lack of management support. To successfully implement ISO 27001, an organisation will need to identify a team to lead and manage the implementation of the standard and to complete the required actions [16]. A further challenge for organisations is limited resources and financial constraints. These challenges can impact the overall implementation of ISO 27001 when organisations may be forced to only implement selected security protocols that are affordable. A workable solution to address this challenge for organisations is to prioritise the areas of security that are most vulnerable to cyberattacks [16].

Literature Review – Challenges and Barriers Implementing ISO 27001

2.6 Continuous Improvement

Continuous improvement is a process for organisations to continuously monitor their cybersecurity, which will identify any current or future risks. Continuous improvement is something organisation need to comply with, within ISO 27001 it's a requirement that must be adhered [17]. The best ways to implement continuous improvement is to establish a culture of continual improvement, this suggests that everyone in the organisation is committing to the continuous improvement [17]. Auditors will expect evidence of continuous improvement for proof that the organisation is continuously improving cybersecurity and systems.

Literature Review – Continuous Improvement

Research Proposal - Deian Rhys Treharne (2120039)

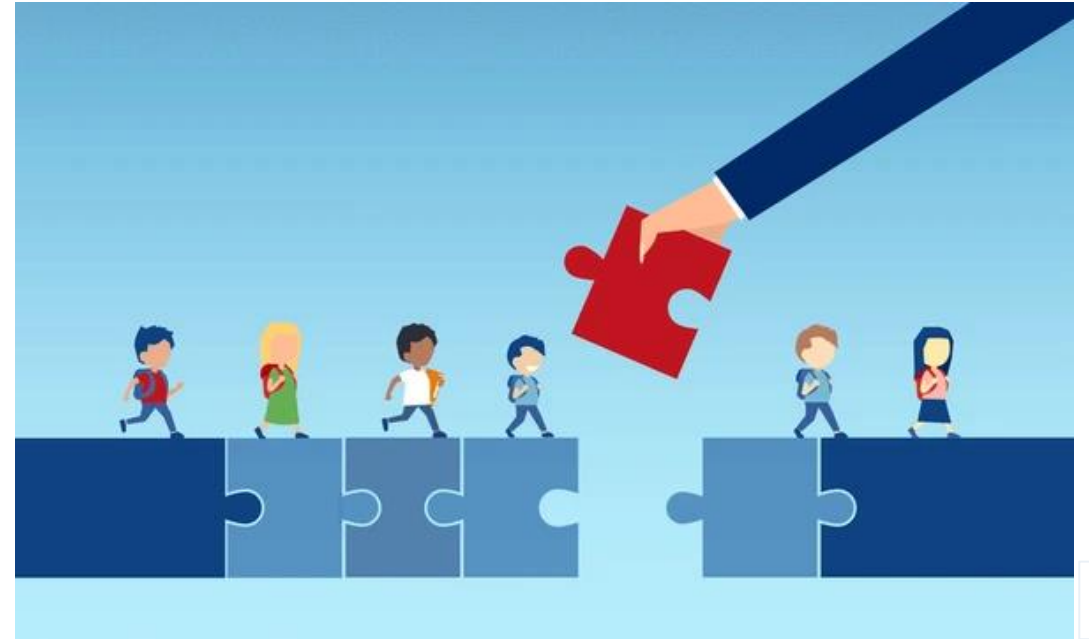
2.7 Risk Management

ISO 27001 recognises that all organisations are different either in size or occupational area, and that all organisations are vulnerable to cyberattacks [18]. A risk management system is required of the standard to mitigate any risks to organisations. Any risks identified from the risk management process are prioritised in order that organisations can protect the most important and key assets (such as finance data, product specifications and physical hardware etc) [18].

Literature Review – Risk Management

Literature Review – Conclusion

- Summary of key findings
- Research gaps
- Implications of the research





Methodology

- Philosophy
- Approach
- Strategies
- Risks/Limitations and Ethical Issues
- Validity, Reliability and Generalisability
- Data Evaluation

Philosophy

Advantages & Disadvantages

4.1.1 Philosophy restructure

The researcher will use two philosophical methods in the research process. These being positivist and phenomenological philosophies. Both philosophies have advantages and disadvantages:

Positivist Advantages and Disadvantages:

Advantages	Disadvantages
Provides objective data [19]	No understanding of the reasoning behind the data collected [20]
Shows patterns and trends [20]	Issues with human behaviour [21]
Generalisable data [20]	Inflexibility [21]

Figure 4 Advantages and Disadvantages of positivist table

Phenomenological Advantages and Disadvantages:

Advantages	Disadvantages
Clear to understand subjective experiences [22]	Researcher induced bias can affect the study [23]
Gain insights around people's actions and motivations [22]	Could be difficult to establish validity and reliability [23]
Provides understands reasoning behind collected data	Time constraints

Figure 5 Phenomenological advantages and disadvantages table

Suitable Philosophy

Research Proposal - Deian Rhys Treharne (2120039)

The researcher will take advantage of both philosophies during this research project. To overcome the disadvantages listed above the researcher must allow time when conducting interviews and surveys this ensures that data is collected effectively. When collecting quantitative data the researcher must provide clear questions for the participants to answer, this can reduce the potential human errors and to avoid disappointing results.

Approach

Advantages & Disadvantages

How to mitigate identified risks

4.1.2 Approach

There are two approaches available to the researcher when conducting the research project. These are deductive and inductive. A deductive approach is best suited to the researcher's hypothesis that the implementation of ISO 27001 does improve organisational cybersecurity. The hypothesis will be tested throughout the research project.

Advantages	Disadvantages
Deductive approach can test specific hypotheses [24]	Limited to exploring new perspectives [24]
Results are replicable and reliable [24]	Deductive approach can be time consuming [24]
Provides clear and structured research protocols [24]	Findings might be subject to researcher bias [24]

Figure 6 Advantages and Disadvantages to deductive approach

To mitigate the disadvantages of the deductive approach the researcher must ensure that plenty of time is allocated to conducting the research, this will improve the quality of gathered results. To avoid the research being bias the researcher must use multiple sources, this reduces the risk of bias by not relying on one source. Collecting data from multiple sources may provide other perspectives compared to used sources.

Strategies

Literature Review

Research Proposal - Deian Rhys Treharne (2120039)

4.1.3.1 Literature Review

The researcher will complete a literature review to analyse published information on the ISO 27001 standard. This will include a review of the ISO 27001 principles, implementation and its effectiveness in enhancing organisational cybersecurity.

Advantages	Disadvantages
Literature review provides a foundation for research to be built upon [25]	Due to new studies being constantly published, this could suggest the current literature review to be outdated [25]
Provides validity and credibility to the research project [25]	Literature review can lead researchers to only research studies that align with their own perspectives [25]
Literature review provides a comprehensive overview of the specific topic [25]	Conducting literature reviews require time and effort [25]

Figure 7 Advantages and Disadvantages to literature review

Case Study

4.1.3.2 Case Study

The researcher will explore organisational case studies to examine security incidents before and after the implementation of ISO 27001. This will provide the researcher with evidence to demonstrate the effectiveness of the implementation of ISO 27001, and to learn how organisations overcome any challenges or barriers during the implementation process.

Advantages	Disadvantages
Case studies can turn opinions into facts [26]	Case studies can have an element of bias due to the researchers' personal feelings towards the topic [27]
Case studies can be conducted remotely [26]	Case studies can be difficult to analyse due to large amounts of data [27]
Case studies can be used at any point during the research project [28]	The results from a case study may not be generalisable due to the nature of the data being specific to the organisation [29]

Figure 8 Advantages and Disadvantages of case studies

Interviews & Surveys

4.1.3.3 Interviews and Surveys

The researcher will undertake a mixed method approach in collecting data. This will include semi-structured interviews and surveys to gather quantitative and qualitative data for this research project.

Surveys Advantages and Disadvantages

Advantages:	Disadvantages:
Selecting the appropriate candidates [30]	Participant answering the survey may be bias [31]
Asking relevant questions [30]	Gathered results may disappoint the researcher [32]
In-depth results [31]	Poor survey design can affect the gathered results [33]

Figure 9 Advantages and Disadvantages of surveys

Interviews Advantages and Disadvantages

Advantages	Disadvantages
Trustworthy Information [34]	Personal Bias [34]
Detailed Assessment [34]	Unpredicted Result [34]
Increasing Knowledge [34]	Disappointment [34]

Figure 10 Interviews advantages and disadvantages table

Risks/Limitations & Ethical Issues

Risks & Limitations

Research Proposal - Deian Rhys Treharne (2120039)

4.1.4 Risks & Limitations

The risks associated with primary research strategies the researcher has selected may be attributable to the disadvantages identified above. To mitigate these risks the researcher will:

- Undertake a pilot survey and semi-structured interviews
- Review articles and published papers in relevant journals
- Review a range of perspectives from academic and professional sources
- Analyse adequate and comparable data sets to enable the researcher to form evidence-based judgements and conclusions

Ethical Issues

4.1.5 Ethical Issues

The researcher will consider ethical issues when planning and preparing the primary research within this project, ensuring that those participating in the research are assured that the research is conducted fairly and ethically. This should include informed consent from the participants, integrity of research anonymity and confidentiality etc. Any data collected must be anonymised to protect participants from any reputational harm.

Validity – Reliability – Generalisability

Validity

4.1.6.1 Validity

The researcher believes that the validity of the selected research strategies are the most suitable strategies available to undertake this research project. The researcher must consider careful sampling of participants. The pilot method can identify and address risks before the main study is distributed to participants. This will allow the researcher to confirm if the research strategies ask the correct questions and the correct participants answering the questions.

Reliability

4.1.6.2 Reliability

Reliability is ensured through using standardised research methods to gather data. If other researchers were to ask the same standardised questions through a survey or interview, this could minimise the possibility of interviewer and survey bias. This would ensure that responses are comparable across different participants. Providing both researchers have followed the standardised methods of gathering data, this increases the possibility of achieving similar findings.

|

Generalisability

Research Proposal - Deian Rhys Treharne (2120039)

4.1.6.3 Generalisability

The researcher's methodology in this proposal may be used in other ISO standards such as ISO 9001. ISO 9001 focuses on the quality management systems (QMS) within organisations [35]. The researcher understands both standards monitor different areas within an organisation, the research methodology can be generalisable.

Data Evaluation Methods

Data Collection

4.1.6.1 Validity

The researcher believes that the validity of the selected research strategies are the most suitable strategies available to undertake this research project. The researcher must consider careful sampling of participants. The pilot method can identify and address risks before the main study is distributed to participants. This will allow the researcher to confirm if the research strategies ask the correct questions and the correct participants answering the questions.

Data Evaluation

4.1.6.2 Reliability

Reliability is ensured through using standardised research methods to gather data. If other researchers were to ask the same standardised questions through a survey or interview, this could minimise the possibility of interviewer and survey bias. This would ensure that responses are comparable across different participants. Providing both researchers have followed the standardised methods of gathering data, this increases the possibility of achieving similar findings.

|



Resources & Planning

- Hardware and Software Resources
- Project Plan (Gantt Chart & Properties)

Hardware & Software Resources

Hardware Resources

5.1 Hardware Resources

A high performing laptop or desktop would be required to carry out this project for example, a laptop with minimum 16GB of RAM and a 500GB SSD. This ensures that the device will be not cause any issues such as the possibility of any data loss. It would be reasonable to invest in an external hard drive. External hard drives can be useful when collecting samples of data such as surveys or notes from interviews. Ideally the researcher would need 1TB storage capacity drive, this will hold many files. For security purposes, the external hard drive will need to be encrypted. This protects the researcher's files and the sources data. Conducting interviews will need require an audio recording device, the specification for this device will need a noise cancelling microphone. This feature can cut out any background noise and produce clear recordings.

Software Resources

5.2 Software Resources

Software resources such as Office 365 would be required for multiple purposes. The usage of OneDrive is important to have a backup of data. By having data stored locally on the researchers C drive is a risk, if the hard drive was to fail all data would be lost. OneDrive allows the user to store data in the cloud, so if there were to be any failures with the device all data will be backed up via the cloud. Office 365 offers products such as Microsoft Word, Microsoft Excel and Microsoft PowerPoint which can all be used to write reports, organise statistical data and present any findings. The researcher can use Microsoft Forms to create, distribute and analyse the surveys electronically. Microsoft Forms allows the researcher to print out copies for those respondents who haven't got access to an electronic device.

Project Plan

Gantt Chart

Gantt Chart Properties



Figure 11 - Project Gantt Chart

The Gantt chart includes the milestones the project will include. Each milestone is measured using the following factors:

Plan Start: Each milestone has a starting point where the researcher will begin that task.

Plan Duration: Plan duration is the amount of time each milestone will need to complete. It's recommended to allocate plenty of time when completing milestones such as collecting data, in case of any possible challenges or delays when capturing the data.

Actual Start: Actual start suggests if there was any reason the researcher could not begin the milestone as described in plan start, actual start can be used to enter the true start week of that milestone.

Actual Duration: Actual duration can be used to show if any milestone took longer than expected.

References

- [1] V. Software, "ISO 27001 – the Information Security Management Standard," Vigilant Software, [Online]. Available: <https://www.vigilantsoftware.co.uk/topic/whatisiso27001>. [Accessed 09 09 2024].
- [2] M. AATHINATHAN, "The Pros and Cons of Cybersecurity: What You Need to Know," LINKEDIN, 22 11 2023. [Online]. Available: <https://www.linkedin.com/pulse/pros-cons-cybersecurity-what-you-need-know-mageshkumar-aathinathan-v5wgc>. [Accessed 11 09 2024].
- [3] X. Qian, "Auto-populating reference Information to augment academic writing," Medium, 28 04 2019. [Online]. Available: <https://medium.com/@xinqian/5-a-literature-review-writing-sample-b431a6b767b>. [Accessed 11 09 2024].
- [4] [Online]. Available: <https://www.shutterstock.com/image-vector/vector-business-man-hand-holding-puzzle-1936996504>.
- [5] T. Barenscheer, "How To Create a Solid Resource Plan: What is resource planning? Why is it important? And steps you can take to become a better resource planner.," Teamly, [Online]. Available: <https://www.teamly.com/blog/what-is-resource-planning-and-why-is-it-important/>. [Accessed 12 09 2024].
- [6] C. Woodward, "Picking the Right Methodology," Simplify Consulting , [Online]. Available: <https://www.simplifyconsulting.co.uk/picking-the-right-methodology/>. [Accessed 12 09 2024].
- [7] L. Goldwater, "Four Tips for Preparing Your References," LinkedIn, 26 01 2021. [Online]. Available: <https://www.linkedin.com/pulse/four-tips-preparing-your-references-lucas-goldwater>. [Accessed 26 09 2024].



Presentation Link

[Recording-20240912_161438.webm](#)

https://uowtsd-my.sharepoint.com/personal/2120039_student_uwtsd_ac_uk/_layouts/15/stream.aspx?id=%2Fpersonal%2F2120039%5Fstudent%5Fuwtsd%5Fac%5Fuk%2FDocuments%2FRecording%2D20240912%5F161438%2Ewebm&referrer=StreamWebApp%2EWeb&referrerScenario=AddressBarCopied%2Eview%2E167a301d%2D0d7e%2D42f6%2Da106%2D55c03ee60d2c