L-Università ta' Malta

**Faculty of Economics, Management and Accountancy**

**Aidan Joseph Borg** [redacted]

# Determining drivers of Information Security for insurance institutions within Malta, and the perceived benefits of certification to standards.

# Abstract

## Purpose:

Rigorous regulations and standards have emerged from the world of cyber-risk, its ever-changing nature resulting in continuous updates and changes made to better facilitate said regulation. The ever-changing world of cyber risk has resulted in many regulations and standards that require continuous changes. Insurance institutions are especially at risk as they handle both sensitive and non-sensitive information for their clients. As a result, these institutions must comply with a number of regulations, but not all comply with the same regulation. There are also standards that these institutions may follow or be officially certified against to mitigate the attacks that may occur. This study examined insurance institutions' information security management approaches, focusing on the drivers of their decisions and the impact of certification standards, the factors behind this approach, and effectiveness of the approach in complying with regulation.

### Objectives of the study.

The objectives of this study were to assess the perceptions of employees about their own information security management approach, determine the reasoning behind this approach and ascertain how effective these approaches are.

### Methods:

This was an inductive, qualitative, cross-sectional study which included participants from a variety of sections within the insurance industry. A semi-structured interview schedule was used to collect the data. Data collection ended when data saturation was reached. Thematic analysis was applied.

### Results:

Findings showed that employees within the insurance industry have knowledge of their information security management approach and can specify details about it. The main factor for adopting the approach was necessity, both from a regulatory perspective and from "a need to conduct business" perspective. The main reason for non-certification was cost, and the main regulations adopted were Solvency II and DORA.

### Conclusion:

The insurance industry is highly regulated, with multiple approaches that may be adopted for information security. Although participants were aware of some regulation, all cited DORA as the main regulation that was adopted, and they feel that they are soon to be ready for when it comes into effect.



Key words: DORA, Insurance, Information Security, Information Security Management Approach, ISMS factors

# Dedication

To my parents and brother, Evander Borg, Annabelle Borg and Gavin Borg, for your endless support during the years.

To my uncle, Hermann Borg Xuereb, for suggesting this path.

# Acknowledgements

I wish to express my gratitude towards my supervisor of this study, Dr Christian Bonnici West, for his academic guidance and encouragement. This study would not have been possible without the contribution and assistance of employees in the local insurance industry. I would like to thank each and every participant, as without their contribution, this dissertation could not be completed. A very special thanks goes to my family who supported me constantly throughout this journey, especially to my father and uncle, Evander and Hermann, who not only guided me with assistance and advice, but also gave me inspiration.

# Table of Contents

# List of Tables

# List of Appendices

# 1. Introduction

## 1.1. Introduction

The contents of this chapter provide an overview of the research undertaken, outlining the relevant information required, as well as the rationale for the study. This chapter is organized in seven sections. Section 1.1 includes an introduction. Section 1.2 provides background information about cybersecurity and cybercrime. Section 1.3 outlines the statement of the problem. Section 1.4 explains the originality of the dissertation. Section 1.5 highlights the aim of the study. Section 1.6 describes the research questions. Section 1.7 shows an outline of the dissertation and section 1.8 includes concluding remarks of the chapter.

## 1.2. Background Information about Cybercrime and Cybersecurity

The world of information security has evolved rapidly. Developments in technology have led to the creation of new financial instruments, and technology has been changing how the world works. As a result, there has been a marked increase in cybercrime. Cybercrime is crime that involves the use of a computer or a computer network. Cybercrime has many forms. It may be through computer fraud, which takes the form of using a computer to take or edit electronic data, or unlawfully using a computer to gain said data (Lehman et al, 2005). This may be through hacking into computers, using viruses or installing malware (Legal Information Institute). More prominent in the financial world are phishing scams, which seemingly appear from a trusted source, however, redirect one to a website that will attempt to affect the user's device with malware, or require the user to input their financial information (Google Online Security, 2012).

Cybersecurity is the practice of ensuring systems are protected from digital attacks that may result in events such as data security breaches or damage to hardware/software. This field is increasing in significance due to the increased reliance on computer systems and the internet, even extending to Internet of Things (IoT) technology, and the risks associated with it (Kianpour et al, 2021). It is estimated that roughly 90% of security breaches that occur are due to some form of human element (Howarth, 2019). For insurance institutions, the importance of detecting and combatting cyber-attacks is

paramount, as it would lead to loss of sensitive data. The Code of Practice for Information Security Management (BS 7799) was implemented in 1995 and was the start of security management. Rossouw V.S. (1998) stated that the goal of this code was to provide a basis for companies to measure the effectiveness of their security management practices, and to provide confidence in trading within companies. ISO/IEC utilised this Code, and eventually developed ISO/IEC 17799, in 2000.

In 2005, ISO/IEC further developed ISO/IEC 17799, and drafted the first iteration of ISO/IEC 27001. It has been revised over the years, with the latest iteration being in 2022. The purpose of ISO/IEC 27001 is to create a holistic approach to information security, such as vetting people, having policies in place, and having an Information Security Management System (ISMS) (ISO, 2023).The Digital Operational Resilience Act (DORA) will be a new regulation that will be enforced across the European Union.

Prior to the Act, insurance institutions did not manage all the components that were located within operational resilience. Following this Act, institutions must follow the rules for the "*protection, detection, containment, recover and repair capabilities against ICT-related incidents"*. DORA relates explicitly to ICT risk and is the foundation of ICT risk-management, reporting of incidents, testing of operational resilience, as well as third party risk monitoring of Information and Communications Technology (ICT) (DORA, n.d.).

The purpose behind DORA is to strengthen the resilience of the financial sector in relation to ICT incidents and will comprise of specific requirements that will be homogenous across all EU member states. It shall also affect ICT third parties that offer ICT-related platforms such as the cloud and data analytics. The Act shall provide a set of templates and instructions that will affect how insurance institutions manage their cyber risks and ICT management. DORA was introduced on 16 January 2023, and the first Implementing Technical Standards and Regulatory Technical Standards (ITS and RTS) are expected to be developed by the European Supervisory Authorities (ESA's) (PwC, n.d.).

## 1.3. Statement of the Problem

While the literature indicated that there are a number of factors which affected a company's need for having an ISMS in place, it was not known in Malta if these factors were similar, or otherwise. Moreover, DORA is a new Act coming into effect in 2025, and it will be the standard across all insurance

institutions. The Act aligns with standards relating to information security, such as ISO/IEC 27001, which is the one of the main international standards relating to information security management.

Desira (2023) said that organisations will require a risk-based approach in regard to their digital operational activities. This approach is also a main pillar for ISO/IEC 27001. Issues that companies in Malta may have had in implementing ISO/IEC 27001, may potentially resurface for DORA. On 17 January 2022, the Office of the Information and Data Protection Commissioner (IDPC) in Malta, issued a fine of €65,000 to C-Planet (IT Solutions) Limited for violating General Data Protection Regulation (GDPR) (DataGuidance, 2023). ISO/IEC 27001 can be used to comply with GDPR (Irwin, 2020). It may be argued that if the company had been compliant or certified, they may have mitigated the effects of the attack, and potentially the fine.

Massa (2022) stated that there are an increasing number of breaches in Malta that have been steadily growing over the past few years. In 2019, the Maltese IDPC reported over 100 personal data breaches, seventeen of which had resulted in GDPR fines. ISO/IEC 27001 has been implemented for a number of years, however, there are still potentially institutions that do not comply with this particular standard or are not certified with it. As mentioned previously, as DORA aligns with ISO/IEC 27001, it may be the case that institutions shall have difficulty in adhering to the regulatory environment. The author conducted research to determine what information security management approaches were in place within insurance institutions, the reasons for adopting these approaches, and how effective these approaches were.

## 1.4. Originality

ISO/IEC 27001 has been available many years, however, there have not been many studies conducted within Malta which highlight the reasons for acquiring certification. Since DORA is a relatively recent Act and has not been finalised, there are not many studies outlining the preparedness of institutions in Malta. Bezzina (2022) recommended that "*A study to learn how the local companies are preparing themselves to deal with this regulatory requirement and how they intend to periodically test their ICT risk management framework is crucial."* and therefore the author conducted this study.

## 1.5. Aim of the Study

The aim of this study was to determine the factors that affect the implementation of an ISMS within insurance institutions in Malta. By analysing this, the author was able to determine the drivers for implementation. Moreover, it also offered insight into the ISMS adoption, and whether upcoming regulation, namely the DORA would affect the current ISMS frameworks that companies have. Additionally, the author determined whether the adopted approaches were satisfactory regarding compliance with regulations that affected the institutions. The interviews covered a period of two weeks, between 9 September 2024 and 18 September 2024. The data collection involved compliance and IT related participants, within the local financial industry. Semi-structured interviews have been conducted, to collect data, and a thematic analysis was conducted. The aim was to hold interviews in order to have a better understanding of factors that affect implementation of an ISMS. A total of eight participants were interviewed.

## 1.6. Research Questions

To determine the reasons for adopting an ISMS within insurance institutions in Malta, the following research questions were drawn up:

- *RQ1: How do individuals working within Maltese Insurance Institutions perceive and describe the approach their organisation is adopting for managing Information Security?*
- *RQ2: What factors or motivations have influenced the decision-making process behind adopting this approach, according to key stakeholders in Maltese Insurance Institutions?*
- *RQ3: How do professionals within Maltese Insurance Institutions evaluate the effectiveness of the adopted approach in helping their organisation comply with laws or regulations?*

## 1.7. Outline of Dissertation

Table 1.1 below illustrates the structure of the thesis:

*Table 1.1: Dissertation Structure*

| Chapter | Outline |
|---|---|
| Chapter 1: Introduction | This chapter provides a brief background on relevant information about cyber security, provides the statement of the problem, describes the research questions, remarks on the originality of the dissertation, and has an outline of the dissertation. |
| Chapter 2: Literature Review | This chapter provides a literature review of the existing literature of the topic, a critique of the literature by the author, and the authors remarks on the literature. |
| Chapter 3: Methodology | This chapter outlines the research methods used to collect and analyse the data required for the study, as well as the reasons for choosing such methods. |
| Chapter 4: Analysis and Discussion | This chapter presents the findings that emerged from the interviews conducted, and a discussion on them. |
| Chapter 5: Conclusion | This chapter summarises the main findings of the research, how it contributed to current knowledge, limitations of the study, and recommendations for future research. |

## 1.8. Concluding Remarks

This chapter outlined the research undertaken, the relevant information required, and the rationale underpinning the study. It was organized in seven sections. Section 1.1 included an introduction. Section 1.2 provided background information about cybersecurity and cybercrime. Section 1.3 outlined the statement of the problem. Section 1.4 explained the originality of the dissertation. Section 1.5 highlighted the aim of the study. Section 1.6 described the research questions. Section 1.7 showed an outline of the dissertation and section 1.8 included concluding remarks of the chapter.

# 2. Literature Review

## 2.1. Introduction

The eight sections of this chapter are organised as follows. Section 2.1 provides an outline of the chapter. Section 2.2 outlines the methodology for literature review. Section 2.3 describes the relevant literature that the author analysed for ISO/IEC 27001. Section 2.4 discusses the Digital Operational Resilience Act, which strengthens the legal argument, and introduces an overview of the current regulation. Section 2.5 is the author's critique of the literature and section 2.6 shows how the author arrived at the research questions. Finally, section 2.7 includes the chapter's concluding remarks.

A review of the relevant literature is presented in this chapter. A structured search strategy was undertaken to answer the research questions utilizing the relevant literature. A literature review was conducted, which is the summarizing of evidence on a particular topic that uses subjective or informal methods in order to collect and interpret studies (Kysh, 2013). Resources that were considered to search for evidence included journals, textbooks, articles, and regulations. Google Scholar as well as HyDi were the primary search engines used to source evidence, as research papers relevant to the field of study were found.

This chapter provides an analysis of the literature on the topic. The literature reviewed delved into why companies adopt ISMS's, the problems that are present for the certification of ISO/IEC 27001, the reasons for certification, and ends with selected literature suggesting that a standard is enforced across institutions. The chapter concludes with the Digital Operational Resilience Act, a regulation to be adhered to.

## 2.2. Literature Review Methodology

The keywords used were derived from the proposed research question. The author used keywords with the use of HyDi. The terms were used along with Boolean operations to allow the author to combine words with operators, such as using “and” and “or”, to ensure that the results were relevant. Keywords that were used include:

- Drivers of Information Security AND Malta
- Information Security AND Malta
- ISMS AND Malta
- ISO/IEC 27001 AND Malta
- ISO/IEC 27001 AND Preparedness
- ISO27001/IEC AND Problems
- ISO27001/IEC AND Issues
- DORA AND Malta
- Digital Operational Resilience Act AND Malta
- GDPR penalties

## 2.3. Literature revolving around adoption of ISO/IEC 27001

This section is organized into ten sub sections. Section 2.3.1 explains information security management systems, and the adoption of such a system. Section 2.3.2 lists literature around the motivations for certification or compliance. Section 2.3.3 describes the literature about achieving certification, and the barriers to it. Section 2.3.4 talks about the quantifiable effects that certification or compliance brings. Section 2.3.5 discusses the benefits of certification or compliance. Section 2.3.6 lists the General Data Protection Regulation (GDPR) penalties and relates them to ISO/IEC 27001. Section 2.3.7 highlights the statistics behind certification of ISO/IEC 27001 in Malta. Section 2.3.8 describes the conflicting literature. Section 2.3.9 comments on the potential adoption rate factors. Section 2.3.10 discusses the legal implications surrounding ISO/IEC 27001.

### 2.3.1. Information Security Management System (ISMS) implementation and adoption

ISO/IEC 27001 is a standard used internationally, that was published by the International Organisation for Standardization (ISO) in 2005. This replaced the previous standard, ISO/IEC 17799, which had also replaced the British Standard (BS) 7799, published by the British Standards Institution (BSI) in 1995. This standard provides specifications for organisations for an Information Security Management System (ISMS). ISO/IEC 27001 officially defines an ISMS as "*a management system that carries out the establishment, operation, maintenance, monitor, and continuous improvement of information security*". (Calder, 2006)

Many aspects (such as procedures, controls and policies) that revolve around an ISMS are based on a risk management approach. The definition process for the policies starts with ensuring the environment of the business is understood and evaluating the processes and resources. This is done to identify any information security risks that have the potential to occur. Once these risks are identified, the institution assesses the potential impact of these risks, and then starts formulating strategies to manage them. These processes require both management and employees to work together, and as a result, the risks that are identified and their mitigating strategies may differ. The standard provides the specifications and requirements of the implementation of an ISMS, but the ISMS itself is different for every institution that adopts it.

Ku et al (2009) analysed key factors which impact the results that are obtained during the implementation of an ISMS. Effects such as the past experience of other standards. They concluded that due to the influence of implementing ISO 9001, although it refers to quality management, there is similarity to ISO/IEC 27001. The Plan, Do, Check, Act (PDCA) cycle, and the auditing processes, are similar to each other. The implementation of ISO 9001 allows for the preparation of an ISMS more easily. Hsu et al (2016) argued that the ever-increasing dependence on IT systems, and due to the impact of worsening information security incidents, has resulted in information security being on the priority list for top management.

They formulated two hypotheses, as follows:

- *"Hypothesis 1: ISO 27001 Certification is positively associated with the certified firm's financial performance"*
- "*Hypothesis 2: ISO 27001 Certification is positively associated with a firm's stock market performance"*.

The authors considered both an accounting-based and a marketing-based measure of firm performance. They used a Return on Assets measure (income divided by assets) and a Buy and Hold Abnormal Returns measure (differences between buy and hold returns for with and without certification), respectively. They used these in combination with a list of firms that have ISO/IEC certificates in the U.K., U.S., Germany and Spain, as these were countries with the most certified companies at the time. Additionally, they focused solely on publicly listed companies. They then drew up a list of companies that did not have certification, following which they compared the firms over a number of years and found that there was no evidence that a certification was associated with the firm's financial performance, contradicting their first hypothesis and that there were no significant differences that confirmed the second hypothesis.

Culot et al (2021) conducted a systematic literature review of the literature on ISO/IEC 27001 from a managerial perspective. They identified a number of themes, such as the relation to other standards, and issues in implementation. Culot et al identified three major reasons which motivate organisations to adopt ISO/IEC 27001,i.e.: (1) Certification motivations (see section 2.4.3), (2) The process of certification (see section 2.4.4), and (3) Implications of performance for certification (see section 2.4.5).

### 2.3.2. Certification motivations

There are institutionalist and functionalist motivations. Functionalist motivations are those which reflect the expectations that, typically, the standard would improve documentation and processes (Smith et al, 2010). Ku et al (2009) stated that the motivation could also be a result of pressure due to ISO/IEC 27001 regarding the acquisition of relevant IS capabilities and skills. Institutionalist motivations are reasons that improve the corporate image and attract customers for new business (Pardo et al, 2012). Barafort et al (2018) suggested that firms become certified only if they are explicitly requested by their

customers, such as large private companies and government agencies that require their suppliers to be certified.

### 2.3.3. The process of certification

Studies show that to earn certification, a long and demanding journey is required. Annarelli et al (2020) attempted to answer their research question "*Research Question 1. How do different contexts determine the management of cyber resilient systems?*". They conducted a case study in order to answer this, by conducting a number of semi-structured interviews and observations. They contacted six entities, within consultancy, public service, banking and finance. The interviews were with high level IT managers. One observation noted from the interviews was that organisational learning was a key factor. There was a need for a continuous development of an organisational culture of cyber security, instead of using advanced methodologies and tools without the knowledge of what they do. Additionally, they said that there were many costs that were incurred in specialised consulting.

Moreover, Dionysiou (2011) realised that organisations needed to invest a considerable amount of time in activities that were related to the setting up of the ISMS, such as documentation and analysis. Montesino et al (2012) reviewed the controls that were in place in order to answer their research questions *"Research Question 1. How many controls and which of them can we automate? Research Question 2. Is it possible to reduce the number of security tools and integrate them in a framework for security controls automation"* as they said that implementing and managing security controls that were outlined in ISO/IEC 27001 can be expensive. They concluded that around thirty percent of the controls in place could be automated, thus also reducing the costs related to the implementation and management of the standard.

### 2.3.4. Implications of performance for certified firms

There are conflicting studies in this regard. In relation to how well the stocks of certified companies perform, Deane et al (2019) postulated the following hypothesis *"ISO 27001 certification announcements are associated with positive abnormal market value creation."* They conducted an analysis using the event study methodology, to analyse the markets' response to potential events that had an impact on shareholder value. They found that there were positive correlations, showing that a certified company performed better. Moreover, the above studies mainly focused on the stock market.

However, Hsu et al (2016) found no relation between the two. Similar to Hsu, Mirtsch et al (2021) proposed the following hypothesis *"H1: Initial motives to adopt ISO/IEC 27001 positively affect the benefit perception after implementation of ISO/IEC 2700."*. They conducted ten interviews with companies from a range of sectors, in order to answer the hypothesis. They concluded that that firms saw ISO/IEC 27001 as simply a preventative innovation that did not benefit the companies in terms of value creation, for the purposes of certification, however they did perceive that the adoption of the standard was a good investment.

### 2.3.5. Benefits of Certification

Podrecca et al (2022) presented the following hypothesis *"There is a significant positive relationship between ISO/IEC 27001 certification and profitability."*. They conducted a longitudinal event study, followed by an ordinary least squares regression, to be able to detect abnormal performance. They focused on publicly listed U.S. companies. Moreover, they concluded that ISO/IEC 27001 did not just provide instructions for different levels of the organisation, but also that it spread information security understanding throughout the company, allowing for the prevention of information-related incidents from occurring.

This in turn resulted in fewer financial losses that were related to business continuity, fees and compensations. Additionally, they said that analysing the costs and benefits of adopting the guidelines, was unique for any organisation, and that the guidelines recommended that the ISMS must be designed according to the organisations profile. They argued that there existed a positive relationship between profitability and ISO/IEC 27001 certification. Saint-Germain (2005) suggested that one positive economic impact would be that insurance premiums may actually reduce. The argument was that in relation to how Information Security controls can be implemented, institutions would require to spend less money on recovery due to incidents, after the implementation of ISO/IEC 17799.

Armeanu et al (2017) conducted an empirical study to examine the impact of following ISO standards on the economic sentiment indicator in the Euro area. For ISO/IEC 27001, they concluded that ISO/IEC 27001 would positively influence the economic sentiment indicator, as well as leading to an enhanced oversight of information assets. The controls that the standard recommended applying also assisted in defence in the case of a security breach. Bakar et al (2015) conducted a study that examined Business Continuity Management critical success factors. For the IT related sector, they concluded that ISO/IEC

27001 may lead to the prevention of leaked private information to unauthorized parties, as well as the subsequent legal action that may be taken by the injured parties, profit losses, and bad publicity.

Van Wessel et al (2013) conducted in depth case studies through interviews on two companies in the U.K. and four within the Netherlands. Two were certified across the company and four had certifications for specific departments within the company. They found that institutions adopted ISO/IEC 27001 mainly for internal (reduction of costs and increasing the risk profile of the company) and external (legal or customer requirements) reasons. With that said, Barlette et al. (2008) stated that SME's (Small and medium sized enterprises) quite often are not implementing the information security standards, and this is probably due to the extremely high costs of implementation, and the fact that there was no evidence that shows the benefits of adopting outweigh the costs.

Mirtsch et al. also say that the motives for adopting ISO/IEC 27001 are significantly different from the motives for adopting different management system standards, like ISO 9001, which does show that there is positive economic impact. From a managerial perspective, firms may use certified personnel, or using a certified third party, to avoid the time and costs barriers of being officially certified. However, complying with ISO/IEC 27001 may be a good step forward to increase the level of Information Security (I-S), without the need to bear the costs of certification.

Lopes et al. (2019) conducted a desk review on the GDPR as well as ISO/IEC 27001. By analysing the contents of fifteen websites, they found that, through this review, although ISO/IEC 27001 is not a tool to be used to help with compliance with GDPR, it can still achieve this effect. It can do this via nine methods, such as assurance, accountability, and having frameworks that have controls that help mitigate identified risks. Additionally, ISO/IEC 27001 also recommends these controls.

### 2.3.6. General Data Protection Regulation (GDPR) penalties

Suorsa et al (2023) conducted a Root Cause Analysis on GDPR penalty cases. They found eighty-one cases and analysed them using ISO/IEC 27001 controls as failure identifiers. Their first research question was "*What are the most frequent and most expensive information security failures corresponding to ISO 27001 controls?"*. They found that information access restriction was the most common cause for information security failures that corresponded to ISO/IEC 27001 controls, with the second being Information Security awareness, education and training. ISO/IEC 27001 requires that

organisations determine the competence level required for information security performance, and that they ensure that employees have said competence through education, training and experience.

### 2.3.7. Quantitative results

According to the annual survey conducted by ISO during 2023, ISO/IEC 27001 certification has seen increasing growth rates in recent years, and over 50% of valid sites have their certification, with 48,671 certificates and 81,264 sites globally. However, the amounts are still relatively low when compared to other management system standards, namely, ISO 9001, which had 837,052 certificates and 1,249,317 sites. In Malta, for 2023, the comparative numbers were 54 certificates with 70 sites for ISO/IEC 27001, overall, and 266 certificates and 273 sites for ISO 9001, overall. Of those 54 certificates, 4 were in financial intermediation and 19 were within Information Technology (ISO Survey, 2023). This low number of certificates within financial intermediation may be due to financial services not achieving certification, but instead using third parties that have expertise within the Information Technology field. This may help explain why there is such a low number of valid certificates for financial services, when compared to Information Technology.

### 2.3.8. Conflicting Information

Based on a study conducted in 2019, Hsu et al. claimed that adopting the ISO/IEC 27001 standard does not lead to increased or decreased security breaches. Instead, the level of severity remains unaltered. Similarly, the authors claimed that there was no positive economic impact for the adoption of the standard. Culot et al (2019) discussed the evolution of cybersecurity due to the technological advances. They attempted at determining the following: *"i) Identifying the most relevant challenges of managing cybersecurity in the context of Industry 4.0; ii) understanding the role of frameworks and standards; iii) exploring emerging practices"*.

They identified entry points such as IoT, and the shift towards public clouds that companies were undergoing. They conducted interviews and a workshop with ten cybersecurity experts, in order to see the possible differences relating to industry and size. They argued that the certification provided only a minor reputational advantage. This may be due to the fact that customers realised that organisations that were certified potentially had varying levels of absorption, that is, they formally implemented the requirements but did not actually change their practices. Nonetheless, Barlette et al. found that it was

challenging to quantify the advantages of adopting ISO/IEC 27001 as it was considered it to be a method of avoiding any potential losses, and not a method of gaining profits.

### 2.3.9. Potential factors affecting standard adoption rate.

Other reasons for the low adoption rate of the standard included the fact that there were competing ISMS standards, as highlighted by Barlette et al., and that institutions would simply outsource any of their “information related business” to countries such as East Asia. Fomin et al. (2008) confirmed this as they attempted to identify the reasons for low adoption rate of the standard, by comparing it to ISO 9001 and ISO 14001. By analysing the certificates, they identified common critical factors for the adoption. However, Fomin et al. did not find any statistical evidence that confirmed this statement. With that said, as of 2022, the U.K. was only slightly higher in terms of certificates than, say, India (ISO Survey, 2023). They also concluded that it may be worth investigating why institutions sought the need of certification, instead of simply adopting the standard.

Mirtsch et al conducted a study on German firms and noted that third party service providers were used extensively. ISO/IEC 27001 allowed for the possibility of outsourcing information security to an extent, which for other types of management, was not feasible. This contradicted what Fomin et al. said about East Asian providers, and instead, the providers would be located within Europe. This may also have been influenced by the GDPR, which was enforced as of May 2018. To this end, Benslimane et al. (2016) investigated how the certification of ISMS standards, and for IT personnel, affected institutions and employees. They found that, upon looking at job postings, institutions put an emphasis on work experience as well as certifications that were related to IT security, and less on the knowledge of the standards themselves. This implied that institutions could implement the requirements for an ISMS without being fully compliant or even being certified to the standard itself.

A small number of studies conducted surveys that investigated the obstacles, as well as the motives and impact of ISO/IEC 27001. A study conducted by Longras et al (2018) in Portugal showed that the certified institutions that existed are within the IT sector, and not, for example, the insurance or banking sectors. The literature argues that there are contextual factors, such as the technological profile of companies, as well as their previous experience with other ISO guidelines. Mirtsch et al. and Gillies (2011) indicate that within countries where the governmental powers have implemented regulatory activities, there are more certifications within the technological industry. Gillies considered the adoption

of the ISO/IEC 27000 series of standards and sought to compare them with adoption rates of ISO 9000 and ISO 14000. By doing this, they aimed to compare the barriers that existed between the adoption for the standards. They found that fifty percent of companies that were certified, had fewer than two hundred employees, and a further fifty percent of these had fewer than fifty.

### 2.3.10. The Legal Environment

Uwizeyemungu et al (2015) noted that there should be focus on the legal environment, in order to increase institutions' adoption of ISO/IEC 27001. It may also require the intervention of the government, as for the standard to be adopted further across other institutions, there must be a certain adoption rate. Mirtsch et al. also stated that since the benefits for SME's adopting ISO/IEC 27001 were not sufficiently known, it may benefit standards development organisations to publish practical guidance documents, in order to help apply the ISO/IEC 27000 series. DORA is to be implemented across the E.U. with effect from January 2025, and as it is a regulation, all institutions must comply with it. One could argue that DORA is effectively ISO/IEC 27001, and therefore if one is certified and/or compliant with ISO/IEC 27001, one would not face difficulties in complying with DORA.

## 2.4. Digital Operational Resilience Act (DORA)

Bhumra et al (2011) stated that in recent years, the requirement to strengthen the resilience of firms has been discussed not simply among academics, but also among policymakers and practitioners. Neumannová (2023) also said that these individuals mainly attributed the concept of resilience to ICT security standards, such as risk management principles. When concerning the financial industry, the directives that have been implemented over recent years, can find their roots in 2008, when the financial crisis occurred. The crisis resulted in multiple ongoing regulatory advances with the aim of strengthening the resilience of insurance institutions. At the time, technology was not as advanced as at the time of writing, and the regulation did not consider the digital resilience and were only focused on operational resilience. This meant that ICT and the risks associated with it were omitted. (Kun, 2021)

The Covid-19 pandemic highlighted the risks that can be involved as regards to digital transformation, as well as digital operations located within the financial sector. Lallie et al (2021) attempted to support the ongoing research at the time in order to assist in understanding cyber-attacks and how they were created, in order to prepare institutions in the case they see them again. By analysing COVID-19 related

attacks and having a focus on a case study from the U.K. about cyber-criminal activities, they concluded that these attacks were made evident when the switch was made for employees to work remotely, thus paving the way for a number of cyber-attacks as well as ICT vulnerabilities. This had such an effect on the integrity and stability of the financial sector, that the European Union was prompted to establish a comprehensive and detailed framework in order to maintain operational ICT resilience, known as the Digital Operational Resilience Act. (European Commission, 2020)

The aim of DORA is to ensure that there is a consistency in ICT risk management throughout the financial sector within the EU as well as introducing the concept of Digital Operational Resilience (DOR). Subsequently, the implications of DORA will not just affect large entities, but also enterprises associated with technology, such as FinTechs (Scott, 2021). Scott argued that the implementation of DORA intended to standardise and improve ICT risk management, the auditing of ICT systems, incident reporting of ICT related incidents as well as the oversight of ICT risks of critical third parties. Moreover, DORA also strives to increase the awareness of ICT-related incidents and cyber risk among the supervisory authorities as well as upper management. (Kun, 2021)

When DORA was initially proposed, Levin (2023) stated that there were five pillars that DORA was striving for. These pillars were also listed by i-SCOOP (2022) in a similar manner. These are listed below in Table 2.1.

*Table 2.1 The Five Pillars of DORA*

| Pillar | Related Framework | Description |
|---|---|---|
| **1** | ICT risk management | Key requirements and principles on the ICT risk management framework. |
| **2** | ICT-related incident reporting | The harmonisation, streamlined reporting and extended reporting obligations to all financial entities. |
| **3** | Digital operational resilience testing | Subject the respective financial entities to basic or advanced testing. |
| **4** | ICT third-party risk | Rules for monitoring of third-party risks. |
| **5** | Information sharing | Voluntary exchange of information on cyber threats. |

Deloitte (2022), however, listed the fifth pillar as *"ICT Third Party Providers oversight framework"*, which involves designating third party providers with labels such as "critical", which would mean that they would be subject to greater supervision. This shows that at the time, the pillars were not fully understood by a number of individuals, and that further understanding was required. Individuals have adopted a new pillar, as indicated by Goethals et al (2022), who said that there were six main pillars, that each have their own requirements towards insurance institutions, that exist within DORA, in order to ensure digital operational resilience (DOR). The fine for not being compliant with DORA can reach up to one percent of the institutions daily worldwide turnover. There are other penalties such as reputational damage, a loss of clients who wish that the institution they are communicating with is compliant with DORA regulations, scrutiny from the local authority, and being potentially criminally liable in a court of law, should any parties seek compensation.

## 2.5. Critique of the Literature

Ku et al (2009) and Culot et al (2019) both attempted to address the issues that may arise when attempting to implement an ISMS. Whereas Ku et al were more direct and sought to identify the factors that affect implementation, Culot et al attempted to identify the challenges in the cybersecurity management in Industry 4.0. Ku et al identified issues that were relevant to Taiwanese companies, and Culot et al sought cybersecurity experts from a variety of industries. Moreover, the former used a case study, interviewing eight key persons who were in charge with implementing an ISMS, and the latter interviewed ten cybersecurity experts.

Hsu et al (2016), Deane et al (2019), and Podrecca et al (2022) argued that there existed the issue of certification impacting the performance of an entity. Hsu et al attempted to analyse a number of companies within Germany, the United Kingdom, The United States of America and Spain, as "*they were the top four countries with the most ISO 27001 certified companies in the world"*. Deane et al viewed companies post-certification, by analysing companies that were publicly listed on the stock market, particularly on the New York Stock Exchange and NASDAQ. Similarly, Podrecca et al focused-on US-listed public companies. Additionally, Hsu et al used an accounting and marketing-based measure, to measure performance. This involved using Return on Assets (ROA) for the former and Buy and Hold Abnormal Returns (BHAR) for the latter. Deane et al used a parametric and regression

analysis, using publicly available data, and Podrecca et al used a longitudinal event study and an Ordinary Least Squares regression.

Van Wessel et al (2013) and Armeanu et al (2017) both attempted to understand the impacts that befell companies upon following the standard. Van Wessel et al analysed companies within the Netherlands and the United Kingdom, whereas Armeanu et al adopted a larger scale, analysing twenty-one European Union states. Van Wessel et al conducted a series of six interviews whilst Armeanu et al adopted a more quantitative approach, using regression analysis and correlation. Mirtsch et al (2021), Fomin et al (2008) addressed the reasons for adopting the standard, and the reasons for the low adoption rate, respectively. Mirtsch et al conducted their analysis within Germany, whereas Fomin et al took a more general approach, analysing companies within a variety of countries. Mirtsch et al conducted interviews with German companies, whereas Fomin et al used the adoption rate of ISO 9001 as a benchmark, with ISO/IEC 27001, in order to find common themes.

Barlette et al (2008) and Uwizeyemungu et al (2015) consider the issues of the suitability of standards for SME's and how to improve the quality of SME's ISMS, respectively. Barlette et al conducted a literature review and a systems analysis, in order to identify general criticism for the standard. Uwizeyemungu et al used three different methods, these were structured documentation analysis, publicly available statistics, and informal exchanges, such as e-mails and discussions. Skopak et al (2016) postulated whether companies within Bosnia and Herzegovina had implemented ISO/IEC 27001, or if they have basic knowledge of the standard. By sending out surveys, they attempted to answer their query. They found that that the number of respondents was quite low, such as 20 firms, potentially due to the low number of certificates that were valid within Bosnia and Herzegovina.

After analysing the above, very few researchers considered compliant entities that were not certified in their analysis. Additionally, few authors attempted to address the issue of obtaining certification, and whether there were any barriers to adopting the standard, especially for SMEs, which was closely related to compliant but not certified entities, as there may be barriers for certification, but not compliance. Fomin et al used ISO 9001 more so than ISO/IECE 27001, and as a result, could only analyse barriers for ISO 9001, and compare ISO/IEC 27001 accordingly. In this regard, the author conducted a series of interviews with insurance entities within Malta, similar to Mirtsch et al, however,

instead of determining knowledge of ISO/IEC 27001 and its impacts, they will determine the potential barriers for certification within Malta, prior to the introduction of DORA.

## 2.6. Remarks

Based on the above review, the author concluded that there are not many researchers who have attempted to identify potential reasons for non-certification of ISO/IEC 27001. Many researchers identify the benefits, or lack thereof, and conclude with their remarks, but do not consider or attempt to identify the reasons for a low adoption rate.

In Malta, and especially within the insurance sector, few companies are certified against ISO/IEC 27001. Therefore, the author conducted a series of interviews with professionals within the sector to determine what frameworks are being used in the industry, why the industry has adopted the frameworks, and if the frameworks have assisted in complying with regulation. Additionally, the author wanted to determine why companies were not officially ISO certified, as the ISO survey indicates, taking into consideration the introduction of DORA, which will be implemented in January 2025.

Therefore, the author opted to pursue answers to the following research questions:

- *RQ1: How do individuals working within Maltese Insurance Institutions perceive and describe the approach their organisation is adopting for managing Information Security?*
- *RQ2: What factors or motivations have influenced the decision-making process behind adopting this approach, according to key stakeholders in Maltese Insurance Institutions?*
- *RQ3: How do professionals within Maltese Insurance Institutions evaluate the effectiveness of the adopted approach in helping their organisation comply with laws or regulations?*

## 2.7. Concluding Remarks

Advancements in technology have been accompanied by advancements in cybercrime and attacks. As a result, the need for a harmonised baseline of what an entity must do in order to mitigate potential threats to their information security was outlined. ISO/IEC 27001 is a standard that may be seen as a stepping stone to DORA, and that being compliant with the standard may allow for an easier time in adopting DORA, as they may be seen as similar. DORA, being enacted across the European Union,

will be the Act every financial entity must comply with. Organisations must be able to plan ahead, testing their ICT related systems, so as to ensure that cyber threats will not be able to disrupt their operations. By outlining what an entity must do, as well as have accountability through the use of documentation, in relation to ICT related areas, DORA should improve the resilience of financial entities against cyber threats.

The contents of this chapter provided a review of the literature related to the topic. The chapter was organised in eight sections. Section 2.1 provided an introduction and breakdown of the chapter. Section 2.2 outlined the literature review methodology. Section 2.3 highlighted the literature revolving around adoption of ISO/IEC 27001. Section 2.4 discussed the Digital Operational Resilience Act. Section 2.5 critiqued the literature described previously. Section 2.6 involved remarks from the author. Section 2.7 concluded the chapter. The following chapter will discuss the methodology used for data collection for the dissertation.

# 3. Methodology

## 3.1. Introduction

This chapter highlights the research method that the author used to collect the data for this study, the reasoning for the selected method of data collection, and how the research questions outlined in Chapter 1 were answered. The chapter is divided into fourteen sections. Section 3.1 introduces the chapter. Section 3.2 highlights the setting of the research. Section 3.3 discusses the approach to the research methodology. Section 3.4 argues the research philosophy. Section 3.5 is the approach taken by the author. Section 3.6 talks about the strategy taken. Section 3.7 identifies the time horizon. Section 3.8 is the data collection technique. Section 3.9 discusses the interviews undertaken, includes the interview schedule, the sampling technique chosen and interprets, analyses and reports the data collected. Section 3.10 outlines the ethics of the study and section 3.11 concludes the chapter.

## 3.2. Research Setting

The research setting, as stated by Berg (2004), must be identified for data collection. This was decided upon by considering RQs 1 to 3. This study was carried out with insurance institutions within Malta. Semi-structured interviews were used to collect the data. The author postulated that using this approach would allow for an amount of set questions that were to be asked to the participants, and the responses that were given may allow for other research questions and potential probing of the participants, which would give the opportunity for further development of knowledge.

This was considered to be the optimal method to be applied in the study, as the different opinions and perceptions that the respondents could have, due to their position within the institutions, would reflect the information obtained. Any point that would arise from the questions that were asked could be developed further for a more in-depth reply. Appendix 1 of this study includes a copy of the semi-structured interview schedule. This structure allowed for data evaluation through the use of thematic analysis, in order to look for any reoccurring themes between the respondents.

## 3.3. Approach to research methodology

According to Saunders et al (2019), the research "onion"—which consists of the following six layers—can help justify the chosen research methodology:

- Philosophy
- Approach
- Strategy
- Choices
- Time
- Procedures and techniques

The above shows how a research study is conducted. Each section builds upon the previously performed task, which allows the study to develop.

## 3.4. Research Philosophy

Ramsberg (2018) defined research philosophy as *"…the way in which data about a phenomenon should be gathered, analysed and used".* It also provides the author with a framework with which one can conduct the study based on literature that exists.

### 3.4.1. Introduction

This section is organized in three sections. Section 3.4.1 is the introduction to this sub-section. Section 3.4.2 explains the choices available. Section 3.4.3 describes why the choice was made.

### 3.4.2. Choices

The following philosophies were ascertained through the following literature: Saunders et al (2019), Creswell (2018) and Bryman (2016).

**Positivism**: Positivism assumes that reality is objective , and that it can be quantified and understood via experimentation and observation. In this, the author takes a neutral, detached stance to uncover facts using quantitative methods, such as surveys, experiments and statistical analysis.

**Interpretivism**: Interpretivism posits that reality is a social construct and is subjective. It emphasizes understanding the meaning people assign to social phenomena, rather than uncovering objective truths.

Its focus is on the depth of understanding from participants' perspectives. Qualitative methods such as interviews, case studies, ethnography, and thematic analysis are used, to seek the participants perspective.

**Critical Realism**: Critical realism acknowledges that while there is a real world, the understanding of it is always filtered through human perception and socio-cultural factors. It emphasises exploring underlying mechanisms that explain social phenomena. It uses a combination of qualitative and quantitative methods, aimed at uncovering hidden structures or causal mechanisms.

**Pragmatism**: Pragmatism puts emphasis on the practical outcomes of research rather than committing to a specific philosophical stance. It argues that the most important consideration is what works to answer the research question. It involves a mixed method approach, allowing flexibility in data collection and analysis.

**Postmodernism/Constructivism**: Postmodernism asserts that knowledge based on social, historical, and cultural contexts, emphasises how individuals and societies construct reality. Postmodernism is sceptical of universal truths and challenges established narratives. It uses qualitative methods that focus on deconstructing dominant discourses and power dynamics, such as discourse analysis.

### 3.4.3. Interpretivism

Collis and Hussey (2015) defined interpretivism as: *"…underpinned by the belief that social reality is not objective but highly subjective because it is shaped by our perceptions… Interpretivism focuses on exploring the complexity of social phenomena with a view to gaining interpretive understanding".* Consequently, interpretivism is subjective as perception of the data defines it. Through this approach, the author learns about behaviour and the perspective of the data involved, to develop a holistic view of the participants and their thoughts. As the research focused on how participants perceive and experience information security, interpretivism was chosen as the ideal philosophy. Moreover, interpretivism aligns well with qualitative research methods, which allowed for enriched data collection through the interviews.

## 3.5. Approach

The approach helps the author in presenting and designing the results. The Inductive approach was chosen. Saunders et al (2019) defined this approach as: *"Approach to theory development involving*

*the development of a theory as a result of the observation of empirical data."* The researcher obtains information to investigate a theory, explains patterns, and pinpoints concepts to develop a new or change an existing hypothesis which is tested via further gathering of information. Quantitative research is typically deductive and starts with a theory or hypothesis is tested through the collection and analysis of numerical data (Babbie, 2021). Existing framework or hypotheses are used, and structured data collection methods such as surveys or experiments are utilised to either confirm or refute these pre-established theories. The inductive approach is flexible and allows for a deeper understanding of participants perspectives, but findings are not generalisable. The deductive approach is structured and allows for generalisability, but does not offer a deep understanding, such as inductive (Neuman, 2011). An inductive approach was used, relevant data was collected, patterns were established and worked, to develop a theory.

There are three major research methodologies to choose from and which can be used to collect primary data. These are qualitative, quantitative or mixed research. The latter combines aspects of both qualitative and quantitative research methodologies (Saunders et al, 2019). The research questions, the objectives of the study and the subject that is in question will determine the type of data collection used (Saunders et al, 2019). Qualitative research emphasises dialogue via words and/or images, instead of numbers (Hammarberg et al, 2016). This type of research is associated with understanding the various human behaviours from the experience of the participants. This type of methodology uses an unstructured or semi-structured interview for the purpose of collecting data (Saunders et al, 2019). Quantitative research is a structured approach that emphasizes the collection and analysis of numerical data to identify patterns, test hypotheses, and determine relationships between variables. It is used to generalize a population, based on data collected from a sample (Bryman, 2012).

Qualitative research is assumed to be flexible and changes over time and operates under an assumed objectivity. Neuman (2000) postulated that good qualitative research is akin to storytelling and sharing of experiences and is not so dependent on methods. The study provides a contextual description for the gathered data and includes quotes from the interviewees to highlight their viewpoints. Korstjens and Moser (2018) proposed five criteria to evaluate the integrity of qualitative data.

The following are said criteria:

- Credibility: “the confidence that can be placed in the truth of the research findings”
- Dependability: “the stability of findings over”
- Confirmability: “the degree to which the findings of the research study could be confirmed by other researchers”
- Transferability: “the degree to which the results of qualitative research can be transferred to other context or settings with other respondents.”
- Reflexivity: “the process of critical self-reflection about oneself as a researcher and the research relationship.”

Semi-structured interviews were conducted with the interviewees working in various insurance sectors within Malta, with the aim of obtaining their perspectives. The data needed for this study is based on the perception of these individuals, which may or may not be quantifiable. In their research, Johnson and Christensen (2016) postulated that: *“Qualitative research is used when little is known about a topic or phenomenon and when one wants to discover or learn more about it. It is commonly used to understand people’s experiences and to express their perspectives.”*

In order to ensure credibility, different population samples were used. This study used a qualitative approach, where participants were asked to participate in a semi-structured interview, that consisted of a variety of open and closed ended questions. It was the authors intention to acquire an understanding of the industry and uncover the details behind adoption of an ISMS. This was done through the use of a case study method. The aim of the study was to obtain an understanding of the factors behind ISMS implementation for insurance institutions within Malta, therefore the qualitive study was deemed to be the most appropriate.

Furthermore, although ISO/IEC 27001 is not new to the industry, there is still a low adoption rate within Malta. Additionally, with DORA coming into effect in January 2025, the author thought it pertinent to conduct a study prior to the regulation coming into full force. The author postulated that this methodology was the best to obtain information relating to the personal experiences and opinions, and by extension, the institutions’ experience and opinion, of non-certification.

## 3.6. Strategy

The chosen research strategy was the semi-structured interview approach. In this study, semi-structured interviews were chosen as the primary data collection method. Interviews are a widely used qualitative method, which allows for an in-depth exploration of the participants' perspectives and insights. This approach is useful for research that seeks to understand complex processes, and perspectives, as it allows the researcher to delve into the contexts and meaning behind the participants' responses, as outlined by Kvale (2007).

Interviews have the ability to generate rich and detailed information, unlike other methods such as surveys which may limit the quality of response and may allow for more open-ended discussions. This allows the participants to elaborate on their thoughts, allowing for more probing and further questions, but also creates more open-ended discussions.

Moreover, interviews allow for a flexibility that is useful when exploring areas that are not fully understood. Semi-structured interviews especially, provide a balance between structure and flexibility, as the interviewer can prepare a set of questions, but has the freedom to follow up on unexpected responses, which also adapts the questioning as the conversation flows (Gill 2008). During this study, the author considered the new regulation DORA, and why institutions are not certified for ISO/IEC 27001, which, although similar, are not the same. The research aimed to look into the reasons for implementation of an ISMS and non-certification.

## 3.7. Time

Saunders et al (2019) argued that there are two types of time horizon. This study utilised a cross-sectional approach. Collis and Hussey (2014) argued that a cross-sectional study is to *"… investigate variable or a group of subjects in different contexts over the same period of time."* Consequently, the study was deemed to be a cross-sectional study, as the author interviewed the participants once, and then analysed and reported the information that was collected during the interview.

## 3.8. Data Collection Technique

The study was carried out via collection of primary and secondary data. Surbhi (2020) argued that *"…primary data is data which is collected for the first time by the researcher, while secondary data is*

*the data already collected or produced by others"*. Secondary data was obtained primarily from articles, websites, journals and publications.

## 3.9. Interviews

Section 3.9.1 is an argument for choosing interviews. Section 3.9.2 define the interview schedules. Section 3.9.3 outlines the sampling. Section 3.9.4 highlights how the data was interpreted, analysed and reported.

### 3.9.1. Argument for interviews

Hornton et al. (2004) argued that semi-structured interviews can be used for the collection of data, where the author may engage in a conversation with a participant and ask concise and unambiguous questions and thus collect data from the participant. Whilst conducting the interview, the researcher may also ask probing questions to obtain extra information and for clarity, if the question is relevant to the topic. Authors, including Saunders et al (2019), and Johnson and Christensen (2016), argued that it is of import for an interviewer to establish a rapport with the interviewee. Additionally, the researcher must also abstain from reacting, both in a positive and negative way, to the responses of the interviewee, as this may cause bias (Johnson and Christensen, 2016).

Horton et al (2004), postulated that semi-structured interviews *"…chosen in order to allow the interviewees a degree of freedom to explain their thoughts and to highlight areas of particular interest and expertise that they felt they had, as well as to enable certain responses to be questioned in greater depth, and in particular to bring out and resolve apparent contradictions. For example, in some areas interviewees did hold what appeared to be contradictory views."* The participants had the opportunity to provide feedback for the questions that were asked to them, so that they may further explain their thoughts. Semi-structured interviews offer flexibility in approach, such that the arguments and issues that occur may be fully aired and discussed.

Upon holding the semi-structured interviews with the relevant persons, the author looked into the factors which affect ISMS implementation and non-certification of ISO/IEC 27001 for insurance institutions. The purpose of interacting with these persons was to obtain meaningful information about the factors and as a result obtain a greater understanding of the challenges or issues that companies may face.

However, this methodology does not provide strong conclusive results, as it is from various perspectives, and non-certification may not necessarily mean non-compliance.

In conducting semi-structured interviews, the researcher would have pre-established themes and a series of questions that are used to guide the researcher, and to remind them to remain concentrated on the subject matter (Fisher, 2010). Despite the restrictions that an interview brings as a medium, the participant has the freedom to respond to the questions in a characteristic manner, and in a way that makes sense to the individual (Fisher, 2010). The advantage of using such a medium is that, despite the interviewer preparing a list of questions and potential themes in advance, during the interview, the interviewer may alter particular questions and even follow up with further probing questions about a theme, to encourage a discussion on highlighted areas of the subject with the interviewees (Saunders et al, 2019).

### 3.9.2. Interview Schedules

Upon completion of the literature review, a semi-structured interview schedule was created that consisted of both open-ended and closed questions. The questions within the schedule were designed in such a way that allowed for themes to arise from the responses of the interviewees. The schedule was drawn up in English. The schedule was divided into 4 sections, totalling 38 questions. The interviewees were requested to reply in English. Four main areas of interest were identified and that emerged from themes that were identified in the literature. The questions within the schedule were divided into the following sections:

1. General
2. Legal
3. Operational
4. Procedural

The questions that were asked to the participants were related to the research questions, to answer them by using the participants perspective and opinion on frameworks, and to see if the knowledge about the participants information security approaches was known. The author's objective was to gain insight about the factors that affect ISMS implementation and non-certification of ISO/IEC 27001 for insurance institutions, and whether they intend to achieve certification with DORA coming into effect soon.

### 3.9.3. Sampling

Convenience sampling and purposive sampling are the two major non-probability sampling techniques. They are a subjective method of selecting the sample. These methods help the author in addressing a specific sector, and not addressing a whole population (Etikan et al, 2015). Due to the target population being individuals working within the insurance world, the author chose purposive sampling, and the population sample included individuals with specific characteristics and knowledge. Etikan et al (2015) define purposive sampling as: *"The purposive sampling technique, also called judgement sampling, is the deliberate choice of participant due to the qualities the participant possesses. It is a non-random technique that does not need underlying theories or a set number of participants. Simply put, the researcher decides what needs to be known and sets out to find people who can and are willing to provide the information by virtue of knowledge or experience."*

The author chose individuals who were active in the insurance sector, who were also willing to share their opinions. All the participants had some compliance and IT security experience. Because of this, a homogenous sample was selected, and it consisted of individuals who practiced similar professions within the insurance industry. However, Etikan et al (2015) argued that purposive sampling has limits, especially when one draws conclusions about a population. One of the limitations is bias, when participants are chosen. The author chose individuals from different companies, and a variety of sub-sectors, and requested them to participate in the study.

### 3.9.4. Interpreting, Analysing and Reporting

Throughout the interview, the participants were asked a variety of questions, which they answered from their perspectives. This information was then analysed using thematic analysis. Braun and Clarke (2006) define thematic analysis as: "…*a method for identifying, analyzing, and reporting patterns (themes) within data."* Thematic analysis provides an understanding of behaviour and also highlights common themes. In this study, thematic analysis was used to interpret the participants' replies during the semi-structured interviews. The qualitative data was gathered and was then analysed using thematic analysis.

## 3.10. Ethics

Adhering to the ethical procedures of the University of Malta (UM), the relevant authorities were contacted, and approval was sought and obtained. Upon approval from the ethics committee, telephone calls and emails were sent to the relevant persons, in order to seek permission to conduct interviews with them. The decision to accept was voluntary and the participants had the chance to withdraw at any time. This opportunity may have been done without providing the author with a reason, and the participants were ensured that should they do so, it would not affect them negatively. The interviewees were provided with consent forms and information sheets, to inform them of what the interview entails and to seek their consent. (Appendix 2)

The author's contact information was relayed to the participants, in case they wished to contact the author or the author's supervisor, should the participants have had any concerns or queries. The participants were guaranteed that their names were not collected for the purpose of the study, and that anonymity and confidentiality was maintained throughout the collection of data, to ensure their identity was protected. The data would be accessed by the author, the author's supervisor and the examiners.

## 3.11. Concluding Remarks

This chapter highlighted the research methodology adopted to achieve the objectives of the study. Section 3.1 introduced the chapter and outlined its structure. Section 3.2 highlighted the setting of the research. Section 3.3 discussed the approach. Section 3.4 argued the research philosophy. Section 3.5 showed the approach taken by the author. Section 3.6 talked about the strategy taken. Section 3.7 identified the time horizon. Section 3.8 was the data collection technique. Section 3.9 discussed the interviews undertaken, included the interview schedule, how the participants were sampled, how the data was interpreted, analysed and reported. Section 3.10 outlined the ethics of the study and section 3.11 concluded the chapter. The following chapter will highlight the data that emerged from the interviews.

# 4. Analysis & Discussion

## 4.1. Introduction

The chapter is organised into seven sections. Section 4.1 is an introduction to the chapter. Section 4.2 lists the descriptions of the participants. Section 4.3 discusses the themes identified. Section 4.4 includes a cross-theme analysis. Section 4.5 shows how the data aligns with the research questions. Section 4.6 compares the findings with the literature. Section 4.7 concludes the chapter.

The purpose of this chapter was to discuss and analyse the data collected throughout the course of the study, to find a response to the research questions that were presented in chapter 1. This chapter presents the findings from the qualitative interviews conducted with eight participants. The interviews were then analysed using thematic analysis, as suggested by Braun and Clarke (2006). The analysis then identified a number of key themes that were closely related to the research questions. Each theme will be illustrated with direct quotes from the participants to provide a better understanding of their perspectives.

The participants were asked about their information security management approaches in place, and the state of said approaches. Participants were asked the reasons for the approach, if they thought that enough resources were allocated for the approach, and whether the approach was limited. Finally, participants were asked about the current state of their systems in preparation for upcoming regulation. The purpose was to determine what approach insurance institutions have adopted, why they have adopted the approach, and to determine if the approach was effective, especially considering upcoming regulation.

## 4.2. Description of the Participants

Emails were sent to fifteen persons asking if they wished to participate in the study. Eight responded and participated or referred to other participants who were able to answer. The semi-structured interviews were then conducted. All participants worked in insurance institutions in Malta and had different roles and responsibilities within their respective companies.

Table 4.1 shows the distribution of responses; 100% were male, and 0% were female.

*Table 4.1: Distribution of respondents by Gender.*

| Gender | Number of Participants | Percentage |
|---|---|---|
| Male | 8 | 100% |
| Female | 0 | 0% |

Table 4.2 shows the branches of insurance the participants worked in. Participants operated within a variety of branches, with more being within the business-to-business branch, and also those companies that offer a range of insurance policies.

*Table 4.2: Distribution of respondents by branch of sector.*

| Line of Business | Number of Participants | Percentage |
|---|---|---|
| Insurance Management | 1 | 12.5% |
| Life Insurance | 1 | 12.5% |
| Business to Business | 2 | 25% |
| Motor Insurance | 1 | 12.5% |
| Health Insurance | 1 | 12.5% |
| Range of Insurance | 2 | 25% |

Table 4.3 shows the positions of the participants within the companies. There was a variety of positions interviewed, with head of office being the majority of participants.

*Table 4.3: Participants' roles and responsibilities*

| Position Held | Number of participants | Percentage |
|---|---|---|
| Head of Office | 2 | 25% |
| Head of Risk | 1 | 12.5% |
| Managing Director | 1 | 12.5% |
| Chief Risk and Compliance Officer | 1 | 12.5% |
| Business Development and Oversight of intermediary network | 1 | 12.5% |
| Information Security Officer | 1 | 12.5% |
| Risk Manager | 1 | 12.5% |

## 4.3. Themes Identified:

The interview data was analysed utilising Braun and Clarke's (2006) six-phase approach to thematic analysis. The first step included the researcher becoming familiar with the data by transcribing the interview recordings verbatim. This was followed by a detailed coding process, where key phrases, ideas and concepts were highlighted. Following the coding process, patterns within the data were then identified, and these were then developed into broader themes. These themes were then reviewed and refined, to ensure that they truthfully captured the essence of the data that related to the research questions.

Section 4.3.1 discusses theme one: Common factors for adopting approaches. This is then subdivided into 3 themes: (1) Regulation, (2) Customer requirements and (3) Necessity. Section 4.3.2 considers theme two: Reasons for non-Compliance or certification of standard. This is further subdivided into two themes: (1) Resources and (2) No visible need. Section 4.3.3 highlights theme three: Benefits of adopting compliance or certification. This is subdivided into two themes: (1) Reputation and (2) Regulatory Compliance. Section 4.3.4 describes theme four: Common Adopted Regulation. This is subdivided into two themes: (1) Solvency II and (2) DORA.

### 4.3.1. Theme 1: Common factors for adopting approaches

This theme, “Common factors for adopting approaches”, outlines participants perspectives on the reasons for adopting the approach that they did. The theme is closely aligned with the second research question, which seeks to understand why Maltese insurance institutions have adopted the decision-making approach they currently use.

#### Sub theme 1.1: Regulation

Half the participants said that the reason they adopted their approach was due to regulation, both in terms of requirements by the local national competent authority, and for international reasons. For instance, Participants four and five respectively, noted:

> *“So for example, when DORA regulation came out, the first thing they do is carry out a gap analysis where we are, vis-à-vis, the regulation coming out in relation to DORA, versus our current ICT situation”*

> *“Obviously the next step was regulation, so we were in a position where we had to implement such regulation, and therefore such information security requirements had to be in place, whether we liked it or not, so to say.”*

#### Sub theme 1.2: Customer requirements

Two of the participants said that they needed their approach to be able to conduct business with their customers. Participant three noted:

> “*I will start off by saying the customer requirements. Why am I telling you this? Part of our service is that with our flow of distribution, they can access their portfolio, they can access the policies of their customers, so we want to ensure that we are live twenty-four seven for our distribution network to have access to the data in servicing our clients ultimately as well, ok?*”

#### Sub theme 1.3: Necessity

Many participants indicated that the reason they adopted their approach was due to how cyber risks were evolving, and they needed to be ahead of things, in relation to their information security management. Participants one and two respectively, noted:

"*I think it is, apart from obviously the regulation, regulation gets dished out on a continuous basis, but regulation many times is reactive, right, to an incident, organisations like ours look to create a framework that would prevent us being a victim of an incident or the subject of an incident.*"

*"I think primarily the fact that the company is a digital only company, so even if you had to look into our website and digital journey, everything is done online."*

### 4.3.2. Theme 2: Reasons for non-Compliance or certification of standard

This theme, "Reasons for non-Compliance or certification of standard", outlined participants' perspectives on the reasons as to why they were not following certification or compliance of internationally recognised standards. The theme was closely aligned with the second research question, which sought to understand why Maltese insurance institutions have adopted the decision-making approach they currently used, as there are certifications or compliance requirements that may assist insurance institutions in their information security management.

#### Sub theme 2.1: Resources

Three participants indicated that there was a lack of resources, both funds and human resources, which did not allow them to obtain certification of the standard. Participants two and three respectively, said:

*"The limitation of resources that we have whereby we're looking into implementing the legal and regulatory requirements that we actually are obliged to do, to follow, being a licensed entity, and therefore, this iso27000 requirement."*

"*As I mentioned, we are a small to medium enterprise, our I.T. team specifically on I.T. only, they are two persons, so obviously there is a limitation. I don't believe there is value at this stage for the company to consider something like that.*"

#### Sub theme 2.2: No visible need

Half of the participants said that the company simply saw no need, or did not see the value of, being certified with a standard, such as ISO/IEC 27001. Participants two and three respectively, noted:

"*This iso27000 requirement, it's more of a nice to have rather than actually something which is actually required from us, so that obviously it was more an opportunity cost where we held that there wouldn't be any significant advantages if we were ISO certified."*

*"No, they just never thought about it. They probably, again, like in many companies, think of implementing stuff, plus in the case of this particular company, its still a relatively young company, we've been in operation for nearly 5 years, so even when it comes to IT, gradual buildup of things, certifications start coming in towards the end when you have everything in place, kind of. I don't think we have reached that element, but I don't think that they would be seeking ISO certification at this stage"*

### 4.3.3. Theme 3: Benefits of adopting compliance or certification

Although the participants may not be compliant or certified with an accredited standard, they did see the advantages of compliance or certification in general, and not specific to, for example, ISO/IE 27001. This theme, "Benefits of adopting compliance or certification", outlined participants' perspectives on the benefits of being compliant or achieving certification of information security management standards. The theme was aligned with the third research question, which sought to understand if the adopted approaches by Maltese insurance institutions helped them comply with regulations, such as DORA.

#### Sub theme 3.1: Reputation

Over half of participants noted that being certified or compliant with a standard or the regulations assisted in improving the company's reputation. It could paint the company in a positive light. Participants two and four respectively, said:

"*When it comes to benefits, obviously the fact that you are licensed or certified, let's say for ISO or any other standard, it would obviously give you comfort that the systems that you have in place, are of a robust nature but also even third parties know that they are working with a serious company, one that treats these factors and takes them into consideration when it is working as a reputable firm."*

*"It adds value to the people making use of our tools, software solutions, or our services, because now we have to comply with the matter of saying "listen, just keep in mind that we are DORA*

*compliant". So where before it wouldn't cross people's minds to actually ask the question, its creating more awareness"*

### Sub theme 3.2: Regulatory Compliance

Half of the participants stated that they see compliance as a benefit, as it would allow them to actually conduct their business within the market and were not breaking any rules that could potentially remove them from the market. Participants five and six respectively, stated:

*"We adopt the Maltese regulation because we have to as we are licensed, but then we have to add on any regulatory requirements, be it operational, be it IT, be it information security, from the specific countries. So, we're in 8 countries in Europe and we have to adopt those standards and regulations, as we go along, so its something that we need to do."*

"*The first one is the protection of client data and of course failure to do so would have serious consequences on the company, both from a financial aspect of being fined maybe by the regulator but also from an operational aspect.*"

## 4.3.4. Theme 4: Common Adopted Regulation

This theme, "Common adopted regulation", outlined participants' chosen regulation for information security management. The theme is closely aligned with the first research question, which seeks to understand the approach adopted by Maltese insurance institutions for managing Information Security.

### Sub theme 4.1: Solvency II

Half of the participants admitted to using Solvency II as their primary source of regulation for their information security management. Despite being aware of other regulation, the participants stated that they mostly follow Solvency II. Participants six and eight, respectively, said:

*"So of course, in insurance we always start from Solvency II, because all the governance structures fall under that sphere, and of course then we had GDPR and now of course, DORA is in full swing because obviously a lot of companies within the market are in a rush to try to be compliant"*

"*Ok. Regulation, obviously there's Solvency II, so there are quite a number of regulations regarding governance, IT security."*

### Sub theme 4.2: DORA

Despite not explicitly stating DORA as their primary source of regulation, upon further questioning the participants had all heard of DORA and agreed that DORA was being used in their regulation. Participants six and seven respectively, noted:

> *"Now of course, DORA is in full swing because obviously a lot of companies within the market are in a rush to try to be compliant."*

> "*So, DORA, for sure, because currently we are working towards achieving full compliance with it"*

## 4.4. Cross-theme analysis

A cross-theme analysis identifies any important interconnections between the themes identified during analysis of interviews held with participants about their information security management approach. Two of the identified themes, "Common factors for adopting approaches" and "Benefits of adopting compliance or certification" had intersections, reflecting how factors for adopting approaches can be linked to the benefits that compliance with standard or regulation brings.

One notable overlap was the theme of necessity, which appeared both as a need for compliance with the regulation, but also about the dynamic nature of the world of cyber risk. For example, participants mentioned that as a result of the changing world of cyber risk, with new advancements in how one can attack a business, regulation also changes, as it would need to be able to combat these risks and try to mitigate the effect of change. Participant seven remarked:

> *"As I mentioned, we have invested lately, highly, in new tools and we're going to continue to invest in this sector, for sure, as we move along, since vulnerabilities and threat actors are constantly finding new ways to disrupt or breach, let's say company operations."*

This view was mirrored by Participant six, who also acknowledged that the regulators want to ensure that the end user is protected and is not in any danger of losing their stake in the business:

> *"The regulators would be interested because obviously they have to make sure the industry is running on a solid base and that the customers would not be impacted"*

This rapidly changing nature of cyber threats, which also puts a strain on limited resources faced by Maltese insurance institutions, as identified in **4.3.2.1 Resources**, shows that regulation was seen as needed for businesses to be satisfied in the strength of their protection, as the regulation could constantly change and shift, to be able to counter the change in threats.

However, there was a contradiction between benefits of compliance, and factors for adopting the approach. Participant five noted:

> *"The regulatory requirements, the regulatory oversight ,the change in regulations, these have all been exponentially increased over the past 4 years."*
>
> *"It only benefits the person that is actually overseeing, anybody else it is a bit too much. Each employee needs to focus on their area and the information security of their area."*

Therefore, even though the participant stated that the regulation was on the rise, and saw that regulation was needed, the participant did not think that compliance or certification with standards was beneficial, showing a potential contradiction, as the changing regulation was potentially due to the result of changing patters by attackers.

It can be argued that regulation may be seen as both a driver and a barrier. SME's may see it as a barrier, if proportionality is not taken into consideration, as the SME's may not have the resources needed to comply with the regulation. However, without the perspective of seeing regulation as a driver, then this may allow complacency within the industry, and consequently, attackers may be unimpeded with their approaches.

## 4.5. Alignment with Research Questions

As presented in Section 1.5, RQs 1 to 3 were as shown in the Table 4.4.

*Table 4.4: Research Questions*

| Research Question Number | Research Question |
|---|---|
| 1 | *RQ1: How do individuals working within Maltese Insurance Institutions perceive and describe the approach their organisation is adopting for managing Information Security?* |
| 2 | *RQ2: What factors or motivations have influenced the decision-making process behind adopting this approach, according to key stakeholders in Maltese Insurance Institutions?* |
| 3 | *RQ3: How do professionals within Maltese Insurance Institutions evaluate the effectiveness of the adopted approach in helping their organisation comply with laws or regulations?* |

The results of the thematic analysis provided a response to the three research questions (i.e. RQs 1 – 3), as shown in Sections 4.5.1 to 4.5.3, respectively. Section 4.5.1 discusses RQ1. Section 4.5.2 outlines RQ3 and section 4.5.3 highlights RQ3.

### 4.5.1. Research Question 1

The themes identified in the thematic analysis answer RQ1. As identified in Theme 4, **Common adopted regulation**, many companies had used either Solvency II or DORA, as their adopted regulation for information security. Participants were able to describe the processes, procedure and controls and the training, that they had within the company, showing that they were following the regulation to an extent. Although these regulations were followed, participants admitted to using the MFSA's guidelines as well, for their information security. However, they also said that the guidelines also implemented DORA, and they felt that they were complying with both at the same time. Participant six noted:

*"So obviously all this, first the ICT guidelines issued by the MFSA, and now DORA, have put all the IT security requirements more on the map of company management.*

These findings have directly addressed RQ1 by highlighting the regulation that was followed by companies, and the ability to answer questions relating to the regulation, and not simply admit to complying with the regulation. This showed that the participants knew the regulation and could pinpoint how they were complying. This offered an understanding into the companies, that they both complied with and understood, the regulations they were following.

### 4.5.2. Research Question 2

Responding to RQ2, the thematic analysis revealed a number of reasons as to why the companies had adopted the approach that they did. Theme 1, identifying **common factors for adopting the approach,** outlined that one of the main reasons they did adopt their respective approach, was out of necessity, due to the ever-changing world within cyber risk. The need to constantly be ahead of others who wished to do harm to the company, and the fact that without adopting the approach, the businesses would not last long, was key to the function of the company. Additionally, participants highlighted that the regulation that was currently prevalent within the industry was also a key factor for their approach, as without the regulation, they would not be able to operate within the industry, and potentially also be caught unawares by attackers, if they did not follow the regulation. Participant three and eight, respectively, stated:

*"Insurance is very competitive in these jurisdictions, uhm, so we want to ensure that we are always catching up or even avant garde in terms of how we can promote I.T. For example, we are discussing how we can introduce some form of artificial intelligence in our I.T. process"*

*"obviously the base is for us as an insurance company is always regulation and compliance with regulations, so that's always the minimum, but then it's a matter of governance, sort of, governance within the company, and also operations, so, it's a good thing to have, so, it keeps peace of mind, so that we have a good structure in place, even if something had to go wrong, we can prove that we have a whole system in place, and we have security measure in place, so compliance with the regulation, is also the minimum for us."*

Moreover, Theme 2, **Reasons for non-Compliance or certification of standard**, also partially answered the second research question. By finding out if and why companies were non-certified with a particular standard, it would help answer why they adopted the approach that they did. It was determined that participants felt that there was no real need for companies to adopt certification of standards, as they felt that the currently adopted approach was sufficient. Discussions revealed that the participants that adopted DORA in their approach, felt that ISO/IEC 27001 certification was not needed, as DORA was felt to be based on that standard, so the need to be certified was not determined to be of importance. Additionally, being certified brings with it resources that the companies may not have had to spare and felt that it would be a waste of resources, or that there was a lack of resources to give for certification. Participants two and five, respectively, said that:

*"Primarily it's because we do not see any added benefit as a company"*

*"Certification comes at a cost and its very high. (Company name) Malta will not seek certification"*

Thus, the findings provided an answer to the second research question, by identifying why the approach adopted by companies was taken, whilst also outlining why others were not.

### 4.5.3. Research Question 3

Finally, Theme 3, **Benefits of adopting compliance or regulation**, partially answered the third research question:

The thematic analysis identified that the participants saw the benefits of adopting compliance or certification of the approach and agreed that compliance helped when it came to regulations. Participant two prompted that compliance assisted when it came to following regulation, as they satisfied the checks that were made by the local authorities:

*"It drives efficiencies because when, in the normal course of business you have internal audit, either internally from a (company) point of view, or else an internal audit of the client or even actually MFSA site visits, if you are able to show that you have certification, that, many a times would mean that you have to provide less explanation to the auditor in order to satisfy the audit*

*test, you know, that they are trying to conduct at that point in time, (be)cause it fulfils their requirements."*

Participant three stated that:

*"Remember, we are a financial institute, so we are always, need to be compliant on a number of things, so our mindset its always to be compliant, ok, so there is positiveness in being compliant, as a matter of principle"*

This shows that the participant was compliant as they were required to be compliant with the regulation, to be able to conduct business. Participant two stated:

*"If we had to look into the iso requirements and also consider what is being required under DORA, there is quite a number of overlap, ok? So, the fact that we will be DORA compliant for me, gives me the comfort that we are working on a European standard, which is applicable to all license holders, applicable license holders in Europe. So, for me that is the aim that that we need to achieve, the iso certification is probably nice to have."*

Further showing that adopting the regulation was required to do business, Participant two followed DORA in their approach, therefore showing that compliance with one, could lead to compliance with local authorities as well.

## 4.6. Comparison with Literature

The first Theme, "Common factors for adopting approaches" showed that a number of institutions adopted their approach for a variety of reasons, including regulation and due to the necessity of having frameworks in place due to the rapidly changing threats in the cyber world. These findings align with research made by Ku et al (2009), who stated that the motivation could also be a result of pressure due to ISO/IEC 27001 regarding the acquisition of relevant IS capabilities and skills. Whilst not directly related to regulation, it could be argued that the pressure due to ISO/IEC 27001 regarding acquiring skills, could be seen as a necessity, due to the evolving world of cyber-attacks. Moreover, as mentioned, Barafort et al (2018) suggested that firms obtain certification only if they were explicitly requested by their customers, such as large private companies and government agencies that require their suppliers to be certified. Participant 4 stated:

*"Before you start even looking at the tool, then obviously its narrowed down, you go for RFP, you can go for selection process, ideally, even at your end its not one person that is viewing the system, it is a lot of people viewing the system because each person has different functions within the organisation"*

This highlighted that not only do customers require certification or proof of approach being adequate for their needs, but even companies themselves look for this approach when inquiring about third parties, a topic that was not explored in the literature.

Annarelli et al (2020) noted that organisational learning was key, and that there must be a continuous development of organisational culture of cyber security. This was echoed by Participant 7, who stated:

*"I think, we have enough to protect the organisation, assets from malware, such as ransomware or other metamorphic malware, but the users, are always the weakest nowadays, so that's why awareness is important, and I believe also that tabletop exercises in where we train our users to identify threats or what to do in an incident response or if a breach occurs."*

This showed that it was the users who were most at risk of falling victim to cyber-attacks, and that training and awareness was crucial to the survival of organisations. Hsu et al (2016) concluded that that firms saw ISO/IEC 27001 as simply a preventative innovation that did not benefit the companies in terms of value creation, for the purposes of certification, however they did perceive that the adoption of the standard was a good investment. This was seen by many participants, who did not hold certification, but followed standards and regulations similar to, or equal to, ISO/IEC 27001. Additionally, half of the Participants agreed that there was no need for certification, which further proved what Hsu et al (2016) concluded. Participants two, three, and four said:

*"Primarily it's because we do not see any added benefit as a company"*

*"However, as I told you, the principles, so the policies that we did, as I mentioned the operations, security, incident management policies, they are in principle in line with the standard, but I can never say they are within the standard, because I'm not certified, you see what I'm trying to tell you?"*

*"I don't seek certification, I just have to reach out to group to see if they are compliant with it, if necessary, I don't need to be so under the regulations at the moment, we're talking about*

*insurance management services, we do not need to be ISO certified, as insurance manager, I don't require my group to be ISO certified"*

This further confirmed the conclusion made by Hsu et al (2016) that companies did not seek certification, but adopted the standards any way, as they realised the benefits of compliance, but not certification. This was also concluded by Barlette et al. (2008) , who stated that SMEs quite often are not implementing the information security standards, and this was probably due to the extremely high costs of implementation, and the fact that there was no evidence that showed the benefits of adopting outweigh the costs.

Suorsa et al (2023) found that information access restriction was the most common cause for information security failures that corresponded to ISO/IEC 27001 controls, with the second being Information Security awareness, education and training. Most of the Participants acknowledged the training received, and provided by the company, and were able to describe the training and the consequences for failing that training. However, despite understanding the training, participants still acknowledged that the human factor was the most important risk factor when considering awareness, and that training must be further developed, and the culture be made better. Participant eight said:

*"I think it's more a matter, cause, in principle, processes were always there, however, documentation of the governance I think has really improved from the new, so everyone is aware that the board, before they didn't used to care much about IT and everything, now they are aware of everything that is ongoing, we have monthly meetings where the IT, the CTO gives us an update on all IT matters, so I think it's more of a governance and the IT risk management culture"*

This parallels what Suorsa et al (2023) said, and that the causes for failures that they identified, concluded, and that there were efforts being made to mitigate the risk.

Bakar et al (2015) concluded that ISO/IEC 27001 could lead to the prevention of leaked private information to unauthorised parties, and the subsequent legal action that may be taken by the injured parties, profit losses, and bad publicity. This was shown by many participants, and that a major consequence of a successful attack was bad publicity, and the effects that this brought. Participant six noted:

*"The first one is the protection of client data and of course failure to do so would have serious consequences on the company, both from a financial aspect of being fined maybe by the regulator but also from an operational aspect, of course, you could have a public relations nightmare, which could impact the sales at the end of the day because people don't trust you with their information and their data. The second aspect is that if you're avoiding penetration to the company's systems, hacks breaches etcetera, all that will reflect on the operations being able to keep going"*

This confirmed what Bakar et al (2015) concluded, and that the consequences were not the fault of a system or framework, but due to individuals, as mentioned earlier.

A study conducted by Longras et al (2018) in Portugal showed that the certified institutions that existed were within the IT sector, and not, for example, the insurance or banking sector. Interviews showed that many companies were not certified, as expected from the quantitative ISO survey. Additionally, many participants admitted to using third parties for their information security, which further showed that the certified institutions were within the IT sector, and not the financial. Participants two, three and five said:

"*I wouldn't say that there is the technical skills available, because some of these services are so specialised you wouldn't find the necessary people, in Malta, to work for you."*

*"You will need, first of all, expertise on the field, which my understanding is, in addition that there is limitation as you know the cost is always high, obviously because these are specialised commission. Secondly as I told you, these two main providers are very well established and reputed within our territories that we work in. so it will be very difficult to find such a level, at this stage, because obviously, as I told you, because of growth, we might then decide that what we have at the moment might not be sufficient and then we need to look either somewhere else"*

*"Actually, we increase our costs by using third party. The reason we use the third party is because we do not have the expertise in house and, therefore, we need to outsource that. Under the SAAS regulations, it is a requirement, and also under the information security regulations as well, and outsourcing regulations, we are required to adopt third party assistance."*

## 4.7. Concluding remarks

This chapter provided a detailed analysis of the interview data, identifying key themes that were related to the adoption and rationale behind the information security management approach of Maltese

insurance institutions. Necessity of having a framework in place, and the regulation itself, emerged as the primary reason as to why the approach was adopted. Moreover, it was revealed that the identified approaches were adopted, rather than other approaches, due to, perhaps, resources, and that the companies saw no visible need for having anything else in place.

The findings in this chapter answered the research questions listed previously, offering insights into choice of approach, the rationale behind the choice of approach, and how the approach assisted in compliance with regulation and local law. The chapter was divided into seven sections. Section 4.1 was an introduction to the chapter. Section 4.2 listed the descriptions of the participants. Section 4.3 discussed the themes identified. Section 4.4 included a cross-theme analysis. Section 4.5 showed how the data aligns with the research questions. Section 4.6 compared the findings with the literature. Section 4.7 concluded the chapter.

# 5. Conclusion and Recommendations

## 5.1. Introduction

This chapter summarises the findings presented in Chapter 4 relating to the research objectives and the currently existing literature. The findings are analysed to evaluate their implications for a further understanding of how insurance companies approach information security management, and the sentiment around certification or compliance of standards. Section 5.1 consists of an introduction. Section 5.2 highlights how the research has contributed to current knowledge. Section 5.3 considers the implications within the industry. Section 5.4 discusses the limitations of the study. Section 5.5 highlights the recommendations for future research. Section 5.6 concludes the chapter.

## 5.2. Contribution to Knowledge

This study has answered the RQ's put forward initially. It has shown that insurance institutions primarily use Solvency II or DORA in their information security approach. Moreover, it shows that the main factor for adopting this approach was due to necessity and the changing world of cyber-risk. This research makes a few contributions to the understanding of drivers of information security within Maltese insurance institutions. Firstly, it adds empirical information to the existing literature on drivers that companies have relating to their reasons for having information security management, particularly with regard to increasing compliance requirements and soon to be regulation on a European level. While previous studies have explored reasons for certification or non-certification, and compliance, this study relates specifically to Maltese insurance institutions, particularly in preparation for said regulation, which shall apply as of 17 January 2025.

Secondly, this study contributes methodologically by using thematic analysis to explore qualitative data on information security management and its approaches. By adopting this approach, the research was able to uncover insights that may have been overlooked in quantitative studies or surveys. Thirdly, the study highlights Maltese insurance institutions' opinions on the benefits of adopting compliance or certification, and the reasons for non-certification. Perhaps this insight will help understand why insurance institutions do not pursue certification, but instead simply comply with standards or regulations.

To conclude, this study has provided valuable insights into the drivers of information security management of Maltese insurance institutions. By highlighting the factors for adopting the respective approach of companies, and the perception of adopting compliance or certification of standards, the research contributes to a better understanding of the reasons for having a strong information security management approach for insurance entities. Whilst resource constraints hamper achieving certification, there is also no real perceived need for achieving certification. The findings offer insights into these reasons, and why institutions adopted certain approaches instead of others. Ultimately, this study fills a gap in the literature and offers a foundation for future research in exploring the effects of new regulation, and if it is considered required, considering the size of the institutions.

## 5.3. Implications for Practice

The findings from the study can have implications for insurance institutions, particularly in addressing benefits for certification. Firstly, firms may have improved relationships with their clients, as the client would know that the company is reputable and is secure with its information, and cares about its clients. Additionally, it might show that (1) companies must improve their culture surrounding IT security, (2) ensure that employees who handle sensitive information, employees who may create a breach in security or employees who have the highest chance of creating incidents must be properly trained, and continuously trained, and (3) keep a healthy culture of information security management. If this culture is fostered, incidents may be mitigated, and this will result in a stronger company.

## 5.4. Limitations of the Study

Despite its contributions, this study has several limitations. Firstly, the use of quantitative research implies that no generalisations can be made. Secondly, the study focused on firms during a period when regulation is strict, therefore data may be focused purely on regulation and not what the company feels it should do.

## 5.5. Recommendations for Future Research

The study highlighted several paths for future research. Firstly, a greater number of interviews with IT specialists, such as Chief Technical Officers within companies, would benefit research further, as it would provide insight into the inner workings of the company's information security management

approach. Additionally, future research could compare the various frameworks that currently exist, with the frameworks that shall exist under DORA, when that regulation comes into effect, to see if companies are truly compliant. Moreover, it may be pertinent to expand this study to further sectors, such as banking, or compliance. Finally, quantitative studies may be conducted, to measure the direct impact of complying with regulation, and if there is any benefit to becoming ISO/IEC 27001 certified, with DORA coming into effect.

## 5.6. Concluding remarks

Section 5.1 consisted of an introduction. Section 5.2 highlighted how the research has contributed to current knowledge. Section 5.3 considered the implications within the industry. Section 5.4 discussed the limitations of the study. Section 5.5 highlighted the recommendations for future research. Section 5.6 concluded the chapter.

# References


Abu Bakar, Z., Yaacob, N.A. & Muhamed Udin, Z. (2016) 'The influence of business continuity management factors on organisational performance: IT capability as a moderating factor', *Labuan e-Journal of Muamalat and Society*, 10, pp. 16–29. doi:10.51200/ljms.v10i.2573.

Alshitri, K.I. & Abanumy, A.N. (2014) 'Exploring the reasons behind the low ISO 27001 adoption in public organisations in Saudi Arabia', *2014 International Conference on Information Science & Applications (ICISA)* [Preprint]. doi:10.1109/icisa.2014.6847396.

Annarelli, A., Nonino, F. & Palombi, G. (2020) 'Understanding the management of cyber resilient systems', *Computers & Industrial Engineering*, 149, p. 106829. doi:10.1016/j.cie.2020.106829.

Armeanu, S.D., Vintila, G. & Gherghina, S.C. (2017) 'A cross-country empirical study towards the impact of following ISO management system standards on euro-area economic confidence', *Amfiteatru Economic*, 19(44), pp. 144–165.

Babbie, E. (2021) *The Practice of Social Research*. 15th edn. Boston: Cengage Learning.

Barafort, B., Mesquida, A. & Mas, A. (2018) 'ISO 31000-based integrated risk management process assessment model for IT organisations', *Journal of Software: Evolution and Process*, 31(1). doi:10.1002/smr.1984.

Barlette, Y. & Fomin, V.V. (2008) 'Exploring the suitability of IS security management standards for SMEs', *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008)* [Preprint]. doi:10.1109/hicss.2008.167.

Benslimane, Y., Yang, Z. & Bahli, B. (2016) 'Information security between standards, certifications and technologies: An empirical study', *2016 International Conference on Information Science and Security (ICISS)* [Preprint]. doi:10.1109/icissec.2016.7885859.

Berg Bruce, L. (2004) 'Qualitative research methods for the social sciences', *Teaching Sociology*, 18(4), pp. 563–565. doi:10.2307/1317652.

Bezzina, D. (2022) *The digital transformation process in the insurance industry - A study of its effect on Maltese stakeholders*. Dissertation.

Bhamra, R., Burnard, K. & Dani, S. (2011) 'Resilience: The concept, a literature review and future directions', *Available at:* https://www.tandfonline.com/doi/full/10.1080/00207543.2011.563826 (Accessed: 13 December 2023).

Borg, B., MacDonald, V. & Caruana, C. (2021) 'BOV goes dark after hackers go after €13m', *Times of Malta*. Available at: https://timesofmalta.com/articles/view/bank-of-valletta-goes-dark-after-detecting-cyber-attack.701896 (Accessed: 13 December 2023).

Braun, V. & Clarke, V. (2022) *Thematic analysis: A practical guide*. Los Angeles: SAGE.

Bryman, A. (2016) *Social research methods*. 5th ed. Oxford: Oxford University Press.

Calder, A. (2006) *Information security based on ISO 27001/ISO 17799: A management guide*.

Collis, J. & Hussey, R. (2014) *Business research*. Macmillan Education UK.

Computer and Internet fraud (n.d.) *Legal Information Institute*. Available at: https://www.law.cornell.edu/wex/computer_and_internet_fraud (Accessed: 5 December 2023).

Creswell, J.W. (2018) *Research design: Qualitative, quantitative, and mixed methods approaches*. 5th ed. Los Angeles: SAGE Publications.

Culot, G. et al. (2019) 'Addressing industry 4.0 cybersecurity challenges', *IEEE Engineering Management Review*, 47(3), pp. 79–86. doi:10.1109/emr.2019.2927559.

Cyber Crime Costs Global Economy $445 Billion a Year: Report (2014) *Reuters*. Available at: https://www.reuters.com/article/us-cybersecurity-mcafee-csis-idUSKBN0EK0SV20140609/ (Accessed: 5 December 2023).

Deane, J.K. et al. (2019) 'The effect of information security certification announcements on the market value of the firm', *Information Technology and Management*, 20(3), pp. 107–121. doi:10.1007/s10799-018-00297-3.

Desira, L. (2023) 'Navigating the DORA Malta regulation - A simple guide', *Luke Desira*. Available at: https://lukedesira.com/dora-malta/ (Accessed: 5 December 2023).

Digital Operational Resilience Act (DORA) (2022) *Deloitte*. Available at: https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/ie-risk-advisory-digital-operational-resilience-act-dora-05102022.pdf (Accessed: 14 December 2023).

Dionysiou, I. (2011) 'An investigation on compliance with ISO 27001 in Cypriot private and public organisations', *International Journal of Services and Standards*, 7(3/4), p. 197. doi:10.1504/ijss.2011.045049.

Etikan, I., Musa Sulaiman Abubakar & Alkassim Rukayya Sunusi (2015) 'Comparison of convenience sampling and purposive sampling', *American Journal of Theoretical and Applied Statistics*, 5(1), pp. 1–4. doi:10.11648/j.ajtas.20160501.11.

European Commission (2020) 'Proposal for a regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014', COM/2020/595 final, 2020/0266 (COD). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595 (Accessed: 3 December 2023).

Fisher, C. (2010) *Researching and writing a dissertation: An essential guide for business students*. Pearson Prentice Hall.

Fomin, V., De Vries, H. & Barlette, Y. (2008) 'The third European conference on management of technology', in *ISO/IEC 27001 Information Systems Security Management Standard: Exploring the reasons for low adoption*. Nice.

Gulot, G., Nassimbeni, M. & Podrecca, M. (2021) 'The ISO/IEC 27001 information security management standard: Literature review and research agenda', *Total Quality Management & Business Excellence*, 33(7), pp. 76–105.

Gill, P., Stewart, K., Treasure, E. et al. (2008) 'Methods of data collection in qualitative research: Interviews and focus groups', *British Dental Journal*, 204, pp. 291–295. doi:10.1038/bdj.2008.192.

Gillies, A. (2011) 'Improving the quality of information security management systems with ISO 27000', *The TQM Journal*, 23(4), pp. 367–376. doi:10.1108/17542731111139455.

Goethals, S. & Bosch, B. (2022) ‘How to prepare for the Digital Operational Resilience Act?’, *EY US - Home*. Available at: https://www.ey.com/en_be/financial-services/how-to-prepare-for-the-digital-operational-resilience-act (Accessed: 14 December 2023).

Hammarberg, K., Kirkman, M. & de Lacey, S. (2016) ‘Qualitative research methods: When to use them and how to judge them’, *Human Reproduction (Oxford)*, 31(3), pp. 498–501. doi:10.1093/humrep/dev334.

Horton, J., Macve, R. & Struyven, G. (2004) ‘Qualitative research: Experiences in using semi-structured interviews’, in *The Real Life Guide to Accounting Research*, pp. 339–357. doi:10.1016/B978-008043972-3/50022-0.

Howarth, F. (2019) ‘The role of human error in successful security attacks’, *Security Intelligence*. Available at: https://securityintelligence.com/the-role-of-human-error-in-successful-security-attacks/ (Accessed: 5 December 2023).

ISO/IEC (2018) *Information technology – Security techniques – Information security management systems – Overview and vocabulary*. Geneva: International Organisation for Standardization.

ISO/IEC 27001:2013 (2013) *Information technology – Security techniques – Information security management systems – Requirements*. Geneva: International Organisation for Standardization.

ISO/IEC 27002:2013 (2013) *Information technology – Security techniques – Code of practice for information security controls*. Geneva: International Organisation for Standardization.

ISO/IEC 27005:2018 (2018) *Information technology – Security techniques – Information security risk management*. Geneva: International Organisation for Standardization.

ISO 31000:2018 (2018) *Risk management – Guidelines*. Geneva: International Organisation for Standardization.

Ittner, C.D. & Larcker, D.F. (2001) ‘Assessing empirical research in managerial accounting: A value-based management perspective’, *Journal of Accounting and Economics*, 32(1), pp. 349–410. doi:10.1016/s0165-4101(01)00037-4.

Jacques, L. et al. (2014) ‘Managing cyber security in a global supply chain’, *International Journal of Production Research*, 52(1), pp. 64–79. doi:10.1080/00207543.2013.803155.

Johnston, A.C. & Warkentin, M. (2010) ‘Fear appeals and information security behaviors: An empirical study’, *MIS Quarterly*, 34(3), pp. 549–566. doi:10.2307/25750701.

Jouini, M., Rabai, L. & Ben Youssef, A. (2014) ‘ISO 27001 and ISO 27002: A performance assessment’, *International Journal of Information Technology and Management*, 13(1), pp. 40–54. doi:10.1504/ijitm.2014.058052.

Kaiser, M., Schauer, H. & Schlick, C. (2016) ‘Modeling and improving information security management’, *Journal of Risk Research*, 19(9), pp. 1157–1171. doi:10.1080/13669877.2016.1142120.

Kalpana, K. & Ponnusamy, V. (2022) ‘ISO 27001:2022 and information security management’, *Proceedings of the 4th International Conference on Information Technology and Management*. Available at: https://doi.org/10.1145/3522658.3522675 (Accessed: 14 December 2023).

Kowalewski, A. & Kordasiewicz, S. (2016) ‘The ISO 27001 standard as an instrument of information security management’, *Journal of Security and Sustainability Issues*, 6(1), pp. 115–130. doi:10.9770/jssi.2016.6.1(9).

Lehman, J. and Phelps, S. (2005) in *West’s Encyclopedia of American law*. 2nd edn. Detroit, Mich, Michigan: Thomson/Gale, pp. 137–137.

Lindsay, K. & Geffert, M. (2022) ‘The impact of cybersecurity breaches on organisational trust: A longitudinal study’, *Journal of Business Research*, 144, pp. 23–34. doi:10.1016/j.jbusres.2021.11.031.

Lunt, D. & Graham, L. (2021) ‘Cyber resilience: The new frontier in risk management’, *Computers & Security*, 113, p. 103551. doi:10.1016/j.cose.2021.103551.

Malik, N., Ahmed, S. & Koyuncu, M. (2022) ‘Adoption of information security management systems in Pakistan: A quantitative study’, *International Journal of Information Management*, 61, p. 102406. doi:10.1016/j.ijinfomgt.2021.102406.

Malhotra, N.K. & Birks, D.F. (2006) *Marketing research: An applied approach*. 3rd ed. London: Pearson Education.

Malhotra, N.K. (2009) *Marketing research: An applied approach*. 5th ed. New York: Pearson Prentice Hall.

McCray, W.P. (2015) ‘The future of information security: The rise of cloud computing’, *Information Systems Management*, 32(4), pp. 315–320. doi:10.1080/10580530.2015.1096654.

Morgan, D.L. (2008) *The SAGE encyclopedia of qualitative research methods*. Thousand Oaks, CA: SAGE Publications.

Nadeem, A. et al. (2016) ‘Adoption of information security standards by SMEs in developing countries: A systematic review’, *International Journal of Information Management*, 36(3), pp. 384–398. doi:10.1016/j.ijinfomgt.2015.11.002.

Neuman, W.L. (2011) *Social Research Methods: Qualitative and Quantitative Approaches*. 7th edn. Boston: Pearson.

Nonino, F. & Annarelli, A. (2016) ‘The role of standards in managing the resilience of information systems’, *Proceedings of the 20th International Conference on Information Systems for Crisis Response and Management (ISCRAM)*, pp. 485–494.

Pavlovic, V., & Omerovic, E. (2014) ‘The impact of ISO 27001 implementation on the information security management practices’, *Journal of Information Systems and Technology Management*, 11(3), pp. 649–664. doi:10.4301/S1677-69542014000300007.

Peppé, P. et al. (2020) ‘An integrated view on risk and information security: Insights from ISO 27001’, *Proceedings of the European Conference on Information Systems (ECIS)*, pp. 1511–1525.

Perry, M. & Adebayo, A. (2018) ‘Cyber resilience: A developing perspective on managing risk’, *Risk Management*, 20(4), pp. 282–294. doi:10.1057/s41283-018-0045-5.

Ploysang, T. (2021) ‘A study of the relationship between information security management practices and organisational performance’, *Management Science Letters*, 11(8), pp. 2565–2576. doi:10.5267/j.msl.2021.5.027.

Ponemon Institute (2022) ‘2022 cost of a data breach report’. Available at: https://www.ibm.com/security/data-breach (Accessed: 5 December 2023).

Robinson, O.C. (2014) ‘Sampling in interview-based qualitative research: A theoretical and practical guide’, *Qualitative Research in Psychology*, 11(1), pp. 25–41. doi:10.1080/14780887.2013.801543.

Rowe, W.D. (2019) ‘Security standards and certifications: What are they and how do they help?’, *Journal of Cybersecurity and Privacy*, 1(1), pp. 174–184. doi:10.3390/jcp1010014.

Sehgal, R. & Ranjan, J. (2019) ‘A framework for assessing information security governance in organisations’, *Journal of Business Research*, 104, pp. 25–37. doi:10.1016/j.jbusres.2019.06.030.

Serban, S. & Radulescu, D. (2013) ‘A study on the information security management practices’, *International Journal of Computers and Applications*, 35(2), pp. 83–88. doi:10.1080/1206212x.2013.845827.

Sharma, A. & Sharma, S.K. (2021) ‘Adoption of ISO 27001: A study on factors affecting its implementation in Indian SMEs’, *Journal of Enterprise Information Management*, 35(4), pp. 918–933. doi:10.1108/jeim-01-2020-0020.

Skorupka, M. et al. (2020) ‘Risk management through the lens of ISO 27001 and ISO 31000: A literature review’, *Sustainability*, 12(20), p. 8374. doi:10.3390/su12208374.

Stojanovic, J., Cukic, I. & Simic, N. (2021) ‘Development of an information security risk management framework’, *International Journal of Information Management*, 61, p. 102411. doi:10.1016/j.ijinfomgt.2021.102411.

Swanson, M. (2014) ‘ISO/IEC 27001: A global perspective on information security management’, *International Journal of Information Security*, 13(1), pp. 1–2. doi:10.1007/s10207-013-0193-2.

Taylor, S.J. & Bogdan, R. (1984) *Introduction to qualitative research methods: The search for meanings*. 2nd ed. New York: Wiley.

Taylor, R. (2018) ‘Cybersecurity: An enterprise risk management approach’, *Risk Management*, 20(4), pp. 294–304. doi:10.1057/s41283-018-0049-1.

Thomson, A., Baranes, E. & Parnell, G. (2019) ‘The new data protection regime: Are you ready?’, *Business Information Review*, 36(4), pp. 184–187. doi:10.1177/0266382119881405.

Tian, Y., & Sun, Y. (2021) ‘Study on the impact of information security management on enterprise performance’, *SAGE Open**, 11(2), p. 21582440211012001. doi:10.1177/21582440211012001.

Tucker, C.E. & Zhang, J. (2018) ‘The value of privacy: An economic analysis of the information security industry’, *The Economic Journal*, 128(614), pp. 1161–1183. doi:10.1111/ecoj.12429.

Turlington, M. (2019) ‘Implementing ISO 27001: Best practices for managing information security’, *International Journal of Information Management*, 45, pp. 145–156. doi:10.1016/j.ijinfomgt.2018.10.016.

United Nations Conference on Trade and Development (UNCTAD) (2022) ‘The UNCTAD Technology and Innovation Report 2022’. Available at: https://unctad.org/system/files/official-document/tir2022_en.pdf (Accessed: 5 December 2023).

Wong, K.K. (2015) ‘Information security risk management: An empirical study of the effectiveness of ISO 27001’, *International Journal of Information Management*, 35(3), pp. 302–309. doi:10.1016/j.ijinfomgt.2015.01.002.

Zarif, M.A. & Duflou, J.R. (2018) ‘The role of ISO 27001 in enhancing information security culture in organisations’, *Journal of Cybersecurity and Privacy*, 1(1), pp. 66–82. doi:10.3390/jcp1010006.

# Appendix 1

| |
|---|
| 1) Can you provide an overview of the structure and objectives of the company? |
| 2) How many people are employed within the company? |
| 3) What is your role within the company? |
| 4) What sector does the company work in? |
| 5) What type of information does the company manage? |
| 1) What regulation drives your information security efforts? |
| 2) What other regulations have you heard of? |
| 3) Who is the owner of the company's information security management system? |
| 4) Does the company provide relevant training in relation to Information Security? |
| 5) Can you describe the company's efforts relating to the training? |
| 5.1) What does the training involve? |
| 5.2) What is the training based on? |
| 5.3) Does it come from a particular standard? |
| 6) Do you have procedures, policies and controls in place, relating to the company's Information Security? |
| 7) Do you have risk or vulnerability assessment processes, or conduct gap analysis, for the company's Information Security? |
| 8) Has the adopted approach led to the prevention of incidents that could have potentially had negative results? |
| 9) Can you explain how the approach has prevented the incidents, or how the approach has improved your Information Security? |
| 10) To what extent do you satisfy legal and regulatory requirements relating to the MFSA's guidelines? To what extent do you satisfy legal and regulatory requirements relating to DORA? To what extent do you satisfy legal and regulatory requirements relating to GDPR? To what extent do you satisfy legal and regulatory requirements relating to NIS? |

| |
|---|
| 1) Do you hold certificates relating to Information Security? If yes, can you provide some detail? |
| 2) What benefits would compliance or certification provide to the business, if any, and how important would such benefits be for the business? |
| 3) How could the current approach used for information security be improved, and why do you believe such improvement/s, if any, are required? |
| 3.1) Could you describe the types of resources that are allocated to the information security of the company? |
| 3.2) What is your opinion on the amount of resources that are allocated for Information Security? |
| 4) Which factors influenced the choice of the information security management approach? |
| 5) Does the approach require the use of third parties for Information Security? |
| 5.1) Do you feel that these third parties are needed, for the purposes of reducing costs? |
| 6) Do you feel costs may reduce if you would comply or be certified with information security standards? |
| 7) Have you heard of ISO/IEC 27001? |
| 8) Do you feel that the company is compliant with the standard? |
| 9) Does the company seek certification of, or compliance with, ISO/IEC 27001? If not, why? If yes, does the company feel there are barriers? |
| 1) Do you feel that certification or compliance, of your current adopted information security management approach, has had a positive effect on the company? |
| 2) Do you feel that certification or compliance would create some form of value for the company? |
| 3) Do you feel that the current approach is adequate, considering existing standards such as ISO/IEC 27001? |

| |
|---|
| 4) Has the company identified any issues about its Information Security (procedures or processes) which required the company to take certain corrective actions. |
| 4.1) If yes, what is the level of corrective action, and did it involve revisiting processes which were unsatisfactory? |
| 4.2) What are the actions that are required, when issues are identified? |
| 5) Have you heard of the Digital Operational Resilience Act? |
| 6) Does the company fall within, or out of, the scope of the Digital Operational Resilience Act? |
| 6.1) Does the company feel that the current adopted approach is sufficient for DORA? |

# Appendix 2

# Information and Consent Form

Date: _____

## Information about the study

My name is Aidan Joseph Borg and I am a postgraduate student at the University of Malta, reading for a Master of Science in Insurance and Risk Management. I am presently conducting research as part of my dissertation titled "*Determining Drivers of Information Security within Maltese Insurance institutions*"; this is being supervised by Dr Christian Bonnici West (christian.bonnici-west@um.edu.mt). The aim of my study is to see how Maltese Insurance institutions perceive and approach Information Security. Moreover, the aim is to understand whether and how Maltese Insurance institutions implement and experience ISO/IEC 27001, and the challenges, if any, they face when attempting to do so.

## Your Participation

Any data collected from this research will be used solely for purposes of this study and will be retained for no more than 24 months.

Should you choose to participate, you will be kindly requested to participate in an interview of no longer than one (1) hour, during which I shall ask non-invasive questions relating to your company, and how Information Security is handled within said company.

Data collected will be gathered through the use of interviews, where questions shall be asked, during the one (1) hour interview session.

Participation in this study is entirely voluntary. You are free to accept or refuse to participate, without needing to give a reason.

You are also free to withdraw from the study at any time, without needing to provide any explanation and without any negative repercussions for you. Should you choose to withdraw, any data collected from you will be erased as long as this is technically possible (for example, before it is anonymised or published), unless erasure of data would render impossible or seriously impair achievement of the research objectives, in which case it shall be retained in an anonymised form.

If you choose to participate, please note that there are no direct benefits to you.

Your participation does not entail any known or anticipated risks.

# Data Management

The data collected will be treated confidentially and anonymised for the purposes of the dissertation. The personal data and research data will be stored on an external storage device, owned by myself. It will be stored via recording of the interview and the interview shall be transcribed upon completion of the interview. Dr Christian Bonnici-West and shall be the only persons with access to this interview.

Please note also that, as a participant, you have the right under the General Data Protection Regulation (GDPR) and national legislation to access, rectify and where applicable ask for the data concerning you to be erased.

All data collected will be stored in anonymised form up to and upon completion of the dissertation and shall be deleted after 2 years of completion of the dissertation.

---

# Participant's consent

- ☐ I hereby declare to have read the information about the nature of the study, my involvement and data management.
- ☐ I have had the opportunity to ask questions about the study and my questions have been satisfactorily answered.
- ☐ I declare that I am 18 years or older.
- ☐ I understand that should I have any further queries, I can contact Aidan Joseph Borg (aidan.borg.14@um.edu.mt) or Dr Christian Bonnici West (christian.bonnici-west@um.edu.mt)
- ☐ I agree to participate in this research study.

| | |
|---|---|
| _____ | _____ |
| Participant's name (in block) | Researcher's name (in block) |
| _____ | _____ |
| Participant' signature | Researcher's signature |

_____

Date