**CISO ROLE IN THE DESIGN AND MANAGEMENT OF AN ENTERPRISE COMPREHENSIVE IT SECURITY PLAN**

Inhalt

[**Chapter 1: Introduction** 4](#_Toc62646889)

[1.1 Background 4](#_Toc62646890)

[1.2 Research Problem 5](#_Toc62646891)

[1.3 Research Questions 5](#_Toc62646892)

[1.4 Aim and Objectives 6](#_Toc62646893)

[1.5 Significance and Justification 6](#_Toc62646894)

[1.6 Organization of Study 7](#_Toc62646895)

[**Chapter 2: Literature Review** 9](#_Toc62646896)

[2.1 Background 9](#_Toc62646897)

[2.2 Chief Information Security Officer 11](#_Toc62646898)

[2.3 COBIT 5 12](#_Toc62646899)

[2.3.1. COBIT 5 Framework 12](#_Toc62646900)

[2.4 Information Technology in Enterprises 13](#_Toc62646901)

[2.4.1 Enterprise Architecture 13](#_Toc62646902)

[2.4.2 Information security 14](#_Toc62646903)

[2.4.3 Information security management: 14](#_Toc62646904)

[2.5 Information Security Policies 15](#_Toc62646905)

[2.6 IT Management 16](#_Toc62646906)

[2.6.1 Management Systems 17](#_Toc62646907)

[2.6.2 Information Security Management System as a part of business processes 18](#_Toc62646908)

[2.8 The CISO’s Role 20](#_Toc62646909)

[2.9 Findings 21](#_Toc62646910)

[2.10 Summary 23](#_Toc62646911)

[**Chapter 3: Research Methodology** 24](#_Toc62646912)

[3.1 Research Approach 24](#_Toc62646913)

[3.2 Research Methods 24](#_Toc62646914)

[3.3 Research Paradigm 24](#_Toc62646915)

[3.4 Rationale behind Selecting Mixed Method Approach 25](#_Toc62646916)

[3.5 Theoretical Frame of the Study 25](#_Toc62646917)

[3.6 A worldview or Philosophical Background 26](#_Toc62646918)

[3.7 Methodological Approach 27](#_Toc62646919)

[3.8 Research Design 28](#_Toc62646920)

[3.8.1 Triangulation Design 28](#_Toc62646921)

[3.8.2 Rationale behind using Triangulation 29](#_Toc62646922)

[3.9 Data Sources and Collection Technique 29](#_Toc62646923)

[3.10 Sampling 30](#_Toc62646924)

[3.11 Data Analysis Techniques 30](#_Toc62646925)

[3.12 Research Limitations 30](#_Toc62646926)

[3.13 Methods of Data Collection 31](#_Toc62646927)

[3.14 Instruments of the Study 31](#_Toc62646928)

[3.15 Data Collection 32](#_Toc62646929)

[3.15.1 Quantitative Data Collection 32](#_Toc62646930)

[3.15.2 Qualitative Data Collection 32](#_Toc62646931)

[3.16 Data Analysis 33](#_Toc62646932)

[3.17 Motivation 34](#_Toc62646933)

[**Chapter 4: Findings and Analysis** 36](#_Toc62646934)

[4.1 Overview 36](#_Toc62646935)

[4.2 Statistical Findings 36](#_Toc62646936)

[4.3 Thematic Analysis 38](#_Toc62646937)

[4.4 Discussion 40](#_Toc62646938)

[References 46](#_Toc62646939)

[Appendix 1: Survey Questionnaire 51](#_Toc62646940)

[Appendix 2: Interview Questions 53](#_Toc62646941)

[Appendix 3: Frequency Charts 54](#_Toc62646942)

[Appendix 4: Frequency Table 65](#_Toc62646943)

# Chapter 1: Introduction

# 1.1 Background

In formation is being considered as the most significant element for the organizations to survive in the current competitive and advanced era. In this regard, the invent of the more sophisticated technologies have resulted in causing the information to flow quite effectively and efficiently throughout the globe (da Silva et al., 2018). Specifically, the availability of information is affecting at each and every level such as it is impacting the decision making of the buyers to select certain product or brand, companies in order to attract wider customer base and compete in the market and the policy makers to take the effective strategic decisions. As a result, the companies are investing heavily to develop such technologies which can help them in attaining significant amount of information, processing it to analyze and extract meaningful outcomes and which can assist them in taking the favorable decisions (Anton and Jones, 2017). In this regard, the companies are not only developing the information technologies but also trying to secure their own information along with the collected data from the outer threats so that the risk of leaking the information could be minimized and could be used in the most significant manner. On the other hand, the risk of information leakage could lead the business towards the interruption, badly impacting the reputation and good will of the company and potential legal consequences which can cause the organization to face huge financial and non-financial losses. As a result, the companies are taking the security of the information technology as the strategic issue of the business rather than only considering it the technological perspective (Catarino et al., 2016).

With the increasing focus and significance of the information technology, the infrastructure is not only enhancing but the risks of cyberattacks are also rising. The companies are trying to secure their own information but also trying to capture larger amount of information regarding the trends, customers, market and obviously for the rival companies as well. Hence, the techniques and infrastructure for attacking the rivals’ information is also becoming a stringer. In this regard, a special post is being created by the corporate sector with the title of Chief Information Security Officer (CISO). The officer is responsible for the information security affairs in the organization. It is not only the internal need of the companies to secure their information rather the external forces also compel the organizations to protect their information by ensuring higher security. For

instance, the legal requirements are there for the organizations to secure their information in a certain way like as per the Network and Information Security (NIS) and General Data Protection Regulations (GDPR) (Hooper and McKissack, 2016). Hence, the role of CISO has become very significant for the success of the business. In this regard, the role and responsibilities of CISO are still not standardized. So, the current research study is aimed at extracting the role of CISO in designing and managing the comprehensive information technology security plan for the companies to protect from the cyber-attacks and also to help in attaining the goals of the business in best possible manner.

# 1.2 Research Problem

The higher connectivity around the globe and digitalization has equipped the information to be an enabler along with becoming a source of competitive advantage for the companies. In order to achieve full advantage of the information asset, this is critical to ensure higher level of cyber security within an organization. Particularly, it is reported by Identity Theft Resource Center (ITRC) that the cyber-attacks for the information assets are becoming vulnerable in quantity and sophisticated in quality with the passage of time (Zandani, 2016). To be more specific, 40% increase in successful cyberattacks is being claimed in the report in comparison to previous year. As a result, the companies hire CISO to devise and manage an IT security plan which can protect the organization from the external threats for the information asset. Bearing the complexity and comprehension of the IT security plans in the companies, and the evolution of the security threats for the companies, the delegation of the CISO is assigned to manage and strategically strengthen the internal and external image of the organization (Peltier, 2013). The current study critically analyses the role of CISO in devising and managing the IT security plan of organizations along with the enablers and opponents for the responsibilities.

# 1.3 Research Questions

The research questions are designed in order to ensure that the directions for the findings of a research study must be designed at very start. Hence, the findings are then tested as per the research questions so the aim of the study is being followed effectively and theme of the research remain same. In this concern, the research questions for the present research study are extracted in light of the problem statement given in the previous section.

* What is the role of CISO in the organizations?
* What are the factors assisting the CISOs to perform their duties for designing and managing the IT security plan in organizations?
* What are the opposing forces in the performance of CISO’s responsibilities?

# 1.4 Aim and Objectives

The fundamental aim of proposed study is consisted of critically assessing the role of CISO in the development and management of the IT security plan for the enterprises. To disseminate the aim, certain objectives are being developed which would be followed throughout the study to ensure the achievement of final goal.

* To critically evaluate the technological trends that have the biggest impact on IT security plan
* To explain the real-time analysis of triage and immediate threats in IT security plan
* To discuss the role of CISO in an organization
* To extract the enablers helping CISO for devising the IT security plan of companies
* To identify the factors that put pressure on the CISO in design and management of an enterprise’s IT security plan

# 1.5 Significance and Justification

The current study is aimed at conducting the analysis to extract the role of CISO in designing and managing the IT security plan in the organizations. In this regard, the literature strand shed the light of the existing research studies and it has explained that despite of the intense need for managing the security issues of the IT security plans in the organizations, the standardization of this job has not yet been decided. Specifically, different organizations are assigning the CISOs with different roles and responsibilities and they are performing those tasks. It is also extracted that the level of the organizations is also changing the responsibilities of CISO. For instance, the CISO at the governmental institution is performing different job while CISO at corporate organizations are being assigned with different role. Hence, by the extractions of findings from the current research study, it could be extracted that what specific role is standardized in the job of CISO for designing and managing the IT security plans of the organizations. Besides that, the findings also provide the enablers and hurdles which are faced by CISO in order to perform the job tasks. Ultimately, the CISOs and organizations would get a chance to analyze and extract the effective role of the CISO along with the enablers and opponents of the job. It will help them in controlling the factors which are causing hurdles while the enablers would be facilitated further. This is the practical contribution of the study which would be provided to the CISOs and organizations. On the other hand, the academic research would also benefit from the findings of the study by providing the methodological directions for the coming researchers to enhance the role of CISO and contribute to its standardization by adding the findings to the literature. So, at the theoretical perspective the contribution of the current study would also be significant.

# 1.6 Organization of Study

The present research study is distributed into five major sections which include introduction, literature review, methodology, findings and conclusion. Mainly, the first chapter opens up the study by introducing the theme of the research. In this regard, the background is provided which lays down the basis for selection of the particular topic along with its significance for the researchers and relevant organizations. The background is then followed by the research problem which discusses the agenda of the issue while explaining the reasons that why this particular research study is being conducted. Further, the research questions are extracted from the research problem of the study. The research questions are designed to explain the pre-determined research criteria for the results of the study to stay connected with the roots of eh study. Moving ahead, the aim and objectives are defined so that the clear image of the study could be provided to the readers. Finally, significance and justification of the current study are provided from the perspective of the practitioners and researchers.

The second chapter provides the review of the relevant research strand. In this regard, the chapter opens up with explaining the introduction which is followed by the conceptual clarification. In this part, the definition of the key terms is provided which are taken from the literature. Moving ahead, the status of information technology in the organizations is provided in light of the literature. The plans and strategies which are followed by the companies to manage the information technology are also discussed so that the existing techniques could be reviewed. Moving ahead, the specific perspective of the CISO is explored by presenting its role in the IT security plan of the organizations. Afterwards, the summary of the literature is provided along with the gap of literature extracted which is aimed to be filled by the current research study.

The third chapter is associated with the methodological design of the present research study. The chapter explains the conceptual framework at first which explains the variables of the study in form of the visual modeling. Then the research methods are presented which are commonly used in the literature and which is used in the current study with the justifications. The methodology chapter also explains about the strategies and approaches which are followed in this study to conduct the research. The sources of data are explaining the modes through which the data is collected which is followed by the specifications the data collection tools. Moving ahead, the sample of the study is explained along with the strategies used to collect the data. The estimation technique is the last part of this chapter which provides the techniques through which the data is analyzed.

The second last chapter explains the findings and results. Specifically, following the methodological measures, the data is collected and then analyzed as per the specified data analysis techniques and then the findings are extracted and presented in the fourth chapter of the study. This chapter also explains the analysis for the findings of the study. The analysis is provided in the light of the literature. The research questions are answered in this chapter by the support of the findings and literature.

Finally, the conclusion and recommendations are provided at the last chapter of the study. The conclusions based on the findings of the research is explained which is then followed by the recommendations. Mainly, the recommendations are provided to the practitioners which are the organizations and the strategic unit and to the academicians which are the researcher in the relevant field who wants to conduct in this area. At the end the limitations of the research are also highlighted.

#

# Chapter 2: Literature Review

#

# 2.1 Background

Nowadays, information is regarded as a basic need, without which organization cannot function (Carr, 2003). Since we live in an increasingly interconnected world, information is much more exposed than other types of basic needs and more vulnerable to attacks (Van Niekerk and Von Solms, 2010). Organizations increasingly recognize that information and related technologies are key business assets (Cadet, 2015), and like any strategic asset, information and related technologies must be effectively managed and protected to ensure business success (Doughty, 2003), because information system incidents may cause business interruption, damage the organization’s reputation and produce legal consequences, which may have a financial impact on the organization (Allianz, 2016). Therefore, over the years, information security methods have evolved from purely technical methods to strategic and business methods (Catarino et al., 2016). With the development of technological infrastructure, information has become more susceptible to numerous threats (Olijnyk, 2015). Therefore, according to the 2016 data breach report released by the Identity Theft Resource Center, it has been determined that the frequency and complexity of cyber attacks have increased. In fact, the number of successful attacks found in 2016 has increased by 40% over the previous year.

Due to the actual complexity and rapidly evolving information security risks, the CISO’s authorization demonstrates the organization’s commitment to the need for dedicated leadership to respond to strategic business commitments and goals (Peltier, 2013). In addition, such as the Network and Information Security Directive (NIS) and the latest laws such as the General Data Protection Regulation (GDPR) have prompted organizations to reconsider their methods and strategies for information security. Market references such as COBIT are also changing their views on the main functions and responsibilities of CISO and information security in the organization's environment, and regard them as the strategic pillar of the organization. The main purpose of this work is to understand the current status of information security in the organization, and how recent regulatory changes affect them, what are the key capabilities and responsibilities of the CISO, and where this function should be positioned in the organization's hierarchy organization Structure.

To achieve these goals, exploratory cross-sectional studies have been conducted to understand events, find new knowledge and evaluate phenomena from another angle. To this end, interviews with experienced consultants and information systems and information security directors in the field of information security have led to the conclusion that the maturity of Portuguese organizations in terms of information security is still low, and it may ultimately be due to the lack of information security in the country. An established safety cultures. On the other hand, the recent changes in regulations are positive for improving the organization and the country’s own awareness of this issue, and help to improve the relevance of the role of CISO. It is generally believed that they should maintain a close and independent relationship with the organization. 'board. It can be concluded that the role and mission of CISO in the organization can be directly related to the understanding of the issue, so that it can be verified that information security is not only an organizational issue, but also a social and cultural issue.

The tradition of technology creation as part of the enterprise strategy has been focused on IT security in past years, growing the need for coherent business/information security strategies. The protection of information is an important part of the organisation when more information needs to be safeguarded so that you can properly respond to security threats in operation. Enterprises are more vulnerable to attacks and other threats and their information storage. These attacks are committed by perpetrators who wish to steal the company's significant information (e.g. intellectual property). Many of the attacks are more advanced and can steal sensitive data. Companies dealing with confidential information should also be prepared to deal with such risks, since information is one of the most critical assets of the business and being equipped with the right information at the right time will result in greater profitability. Companies are increasingly perceived with regard to information and associated technology as essential organisational assets to be handled and managed effectively.

IT has become an important resource for all enterprises, and is becoming increasingly important in all fields of business and public relations. There is a growing need to reduce information risks. This included information security and threats to IT-related assets. Protection of information plays a crucial role in routine activities to secure information, one of the organization's most valuable assets. Protection of knowledge is an entrepreneur and is strictly connected to stakeholders' reliability. It is a strategic advantage for the organisation regardless of whether market risks are to be addressed or value added. Security is also essential to the company's day-to-day operations as it needs to safeguard and make accessible the privacy and confidentiality of its information. In the subsequent year, cybercriminals have become more sophisticated and co-operative. To counter these challenges, ISO experts have to consider the following five patterns:

* Unintended consequences of state intervention
* Big data will cause big problems
* Mobile applications and the Internet of Things (IoT)
* Cybercrime triggers a perfect threat storm
* The skill gap becomes the abyss of information security.

Well-trained information security professionals are important for organisations in order to respond to threats and solutions. Many smaller businesses can't justify setting up or maintaining a dedicated information security unit. These organisations typically use general operations or financial teams, especially those without external compliance requirements, to host the main safety information plan which may cover technological, physical and personal protection, It's really good effect. Variously.

# 2.2 Chief Information Security Officer

CISO manages risk, runs protection, physical security and balances business and security objectives. It is also part of the management of information security, which comprises:

* Executive management
* business Administration
* CISO/Information Security Manager (ISM). CISO is a senior management staff of the company, who is responsible for the vision, strategy and plan of the company and for ensuring that information technology and assets are secured against non-users. Approval. One of the objectives of this role is to minimise information and IT risks. CISO should direct workers in improving risk management. All information security processes are established, developed, implemented and managed by these staff. CISO is also a big part of decision makers for security details, including:
* CISO;
* Information Security Steering Committee (ISSC);
* ISM;
* Enterprise Risk Management;
* Business owners. The position of the CISOs has previously been based only in the definition of technical standards and security policies, the validation of security checks, and customer protection.

Today, the organisations understand that CISO's priorities are gradually changing because cyber threats are inextricably connected with its innovation and growth strategies. CISO provides a new capability, such as leadership, which requires strong communication skills to collaborate, work with and communicate in and outside the organisation, with the boards and managers of different departments. This relationship is essential for the achievement of growth and innovation between CISO and the company.

CISO is responsible for the coordination of information resources confidentiality, honesty and availability. One of the core competencies of CISO is that of translating business problems and solutions, such as CEO, CIO, manager of business, etc., into a language which business people can understand. It is a key skill because, to support the business mission and the vision, CISO must build relationships with all business partners. CISO needs to train its staff to build a new culture of information security that everybody embraces.

# 2.3 COBIT 5

The COBIT 5 framework and solution embraced by many companies who want to play or sustain the role of CISO will be presented in this section. The solution is a COBIT 5 information protection guide for IT and other relevant parties. The solution is COBIT 5.

## 2.3.1. COBIT 5 Framework

COBIT 5 represents a structure which contains comprehensive guidance on company IT management and governance enabling factors. This system consists of a collection of good IT governance practices. It has been released by the ISACA in April 2012. It was also published. In this system, the management process is guided by management needs and input from the management process is given to determine the course of implementation, and/or whether adjusts are needed. The management process is guided by business needs.

COBIT 5 incorporates other main structures, standards and tools such as the International Organization for Standardization (ISO) Information Technology Infrastructure Library (ITIL) and its associated standards. The ISACA Global COBIT Survey 2016 results indicate that three-quarters of the participants said that COBIT 5 would help them address business issues outside of corporate IT administration.

Moreover, COBIT 5 was found to exploit existing practises and global thinking to maximise value for the stakeholders for companies of all sizes. COBIT 5 supports organisations, whether they are a corporation, a non-governmental organisation or the public sector. COBIT 5 is primarily used by managers and consultants in the fields of audit, compliance, IT, governance, security & risk management.

In order to meet the COBIT 5 information protection guidelines, the investigation focuses on information security. This guide has many market advantages, such as:

* Reduce uncertainty and rentability. The alignment of information security principles and good practises was strengthened and simpler to do this.
* Boost user fulfilment. This is done by the findings of information security
* Reduce effect by reducing safety accidents in information
* Enhance the incorporation of security of business information;
* The security of information increases the administration of costs.

# 2.4 Information Technology in Enterprises

Business processes continuously process information to bring effective results to the company (Chaudhary et al., 2017). Basically, these processes follow the principle of information, where input is provided on information based on decisions or business strategies. Second, the information input is processed according to the information installed in the operating tool. Finally, the results are generated based on the information inserted by the company. Basically, the data is collected at the first point of processing, and the analyzed data becomes useful information so that the company can use it in strategy formulation (Bessen, 2017).

Information systems have completely shaped the way business is conducted because it enables companies to access customers from all over the world, and enhances competitive advantages and improves strategic business management. In this case, organizations are making implicit and explicit decisions about the needs and use of information. The central issue of information use is related to cost and benefit analysis based on the expected results of the business. Generally, Cupial et al. think. (2018) The company is a major customer of information that makes business processes more efficient.

## 2.4.1 Enterprise Architecture

Architecture is the fundamental organisation of the system expressed in its elements, its relationship to the environment and its architecture and evolution principles. Enterprise Architecture (EA) is the whole architecture at organisational level. EA is a set of coherent concepts, models and methods for the design and execution of an organisational, corporate, information and technology structure of a company. The EA mechanism can enhance accountability, inform control and decision-making, and help IT management. Each company needs to do the right thing with minimal risk of cost savings and benefit. In order to achieve these targets, EA supports the IT management of the company. EA is important to the company, as we have seen, but what is its objective? The response is simple: an organisational understanding; creation of processes, goods and services for business purposes; optimization of operations; optimisation of organisation resources (including personnel) and consistencies at all levels of organisation.

## 2.4.2 Information security

The information security framework ISACA describes as "ensure that the company's internal protection of information from disclosure to unauthorised users (confidentiality), incorrect modification (integrity), and lack of access rights when necessary (availability)" Among other factors, the procedure is defined in protecting information against unauthorised access, use, recording, alteration, disclosure, etc. Info security is an important research concept since CISO is responsible for overall governance of information security for businesses.

## 2.4.3 Information security management:

The ISO 27000 standard defines information security as the process of “protecting the confidentiality, integrity and availability of information” (International Organization for Standardization, 2014). Its main task is to ensure business continuity and reduce damage to information security incidents through restrictions. influences. (Von Soms, 1998). Information security management that is limited to information technology and processes alone is not enough to give global influence in large organizations (Sajko et al., 2011). Information security governance is defined as the process of defining, establishing, and maintaining management structures and processes that support the alignment of information security with business objectives, while at the same time being consistent with the law, through the adoption of policies, control measures, and the establishment of roles to formulate appropriate regulations. And the responsibility to support better risk management in the organization (Bowen et al., 2007).

The process of organizing information security in an organization must consider various factors, such as its tasks, composition, authority, responsibilities, roles, communication channels, coordination, and position in the organizational structure (Peltier, 2013). When defining information security management guidelines, Basie von Solms proposed 13 dimensions in 2001. No matter how they are organized, they must work together to create a secure environment (Von Solms, 2001):

* Corporate strategy and governance dimension;
* Organizational dimension;
* Policy dimension;
* Best practices dimension;
* Ethical dimension;
* Certification dimension;
* Legal dimension;
* Insurance dimension;
* Human dimension;
* Awareness dimension;
* Technical dimension;
* Metric dimension; and
* Audit dimension.

Therefore, information security must be understood and managed as a multidimensional issue (Von Solms, 2001), and must be treated as a responsibility of management and corporate governance. The development of risk management, reporting and leadership responsibilities

should enable the organization to have an appropriate level of information security maturity (Posthumus and Von Solms, 2004).

# 2.5 Information Security Policies

The principal purpose of the Protection Strategy is to ensure an effective basis for security of information, identify employees' roles and responsibilities in protecting information assets and illustrate how important organisational communications are to protect them. The first step in reducing the possibility of unacceptable use of the information assets of an organisation is the implementation of a security policy. With a security plan worker not only engage completely in the work of the company to secure their information resources but also reduce the likelihood of security violations caused by "human factor" mistakes. A safety mechanism is built to recognise, describe and document the organization's valuable assets and how they are to be safeguarded. It offers a consolidated document containing all information-on-information resources protection. (Danchev 2003, Greene 2014.)

# 2.6 IT Management

The global department of technology management creates an organisation for today and tomorrow. It is a connection to the "Engineering, science, and management discipline planning, development and implementation of technical capabilities to shape and achieve the organization's strategic and operational goals" (cited in Ettlie 5). "Tendency is the fundamental characteristic of technology management, which involves creativity and the duplication of sufficient resources and routines in order to effectively realise technical capabilities that meet strategic goals and business needs. It is an evolutionary measure of organisational capacities (McCarthy 739). Changing market practises, which typically include using emerging technology, usually achieve organisational adaptability. The technology includes usually information systems like Optiva, Peoplesoft, Oracle, SAP and other ERP systems. The information system allows operations to be more effective and productive by eliminating redundancies, standardising operations, preserving past job documentation and recognising potential opportunities. Thousands of implementations are currently in operation. Although these systems provide substantial changes and provide multiple prospects for potential

development, in the next decade any system will have to be revamped to continue to achieve corporate adaptability.

IT management is defined as a mechanism through which the security of data confidentiality, the availability of authorized users and its core integrity can be ensured. The main goal of information security management is to ensure business continuity and minimize the damage caused by threats to information security (Luftman et al., 2017). In this sense, another term is used in the literature, called information security governance, in which a company’s management defines, develops and manages a specific process structure to support the organization’s goals and security. Information (Soto Acosta et al., 2018). In addition, governance also involves the introduction of laws, regulations, and regulations to ensure better management of constant risks and threats to the company's information system. In this regard, it is extracted that the IT management of the enterprise must be related to the organizational tasks, structure, communication, environment, authority, and employee responsibilities and roles. The literature specifically explains the guidelines to be followed in the information security management plan, such as corporate strategy and governance standards to be considered when establishing an information security plan. In addition, organizational and political aspects are also critical to the success of an enterprise’s IT security program, because the scope must be aligned with the organizational aspects. However, it is also necessary to align the safety plan with the code of ethics to protect stakeholders from the adverse effects of the plan (Ávila and Garcés, 2017). Therefore, it can be concluded from the discussion of the literature that information security should be viewed as a multi-directional decision involving all major and minor aspects of the organization.

## 2.6.1 Management Systems

According to Rollenhagen and Wahlström (2013), a management system is a tool that can help define how to perform organizational management based on roles and responsibilities, organizational planning and monitoring. The author further divides the management system into two parts: formal and informal. The author suggests that dividing it into two parts can be regarded as an ideal management system, and then must face the way the planned management system works in practice. The formal part of the management system usually exists in the form of

documents and is usually developed through planned work according to a predetermined structure (Rollenhagen & Wahlström, 2013).

Subsequently, through inspection, it is possible to study to what extent the defined process is maintained and whether the purpose of the management system meets the established goals. The informal part is usually related to organizational culture and represents the way people in the organization work in practice (Rollenhagen & Wahlström, 2013). Rollenhagen and Wahlström (2013) pointed out that organizational culture usually develops spontaneously, although people sometimes try to guide the culture, and the culture is affected by the surrounding world, influencers, technological progress and other factors. (Rollenhagen & Wahlström, 2013). However, if the formal and informal systems are very different, problems will arise (Rollenhagen & Wahlström, 2013). Within the organization, a safety-specific management system has been developed to develop and maintain a good safety culture (Rollenhagen & Wahlström, 2013).

LIS (see Figure 1) is a management system that provides guidance on how to manage or manage organizational information security (MSB, 2018a). The system was developed by a working group composed of professionals and researchers and MSB (MSB, 2018a).

 We chose to focus on the existing literature based on LIS because it outlines the necessary components to prevent cybersecurity incidents. In addition, we believe that the management system is important because it was developed by the Swedish Civil Emergency Agency (MSB), and according to the authority’s regulations, the management system is applicable to all organizations regardless of their size or location. When organizations perform information security tasks, they usually rely on the best practices described in the information security internal management system standards (MSB, 2018a). LIS is based on the SS-EN ISO/IEC 27001 standard, and all information security standards are compiled in the 27000 series (MSB, 2018a).

Importantly, LIS is adjustable, which means that organizations can adjust it to better meet their specific needs. LIS consists of four parts: identification and analysis, formulation, use, tracking and improvement, and the mutual influence of each part, similar to a chain effect.



## 2.6.2 Information Security Management System as a part of business processes

In the modern world, organizations and their business operations rely heavily on different information systems, whether they are public or private. It is no exaggeration to say that our entire society depends to some extent on information systems and their security. For example, from the electric alarm clock from getting up in the morning to turning off the lights at night until we fall asleep, our modern lifestyle depends to some extent on technology. Even at night, there are some systems that can control our sleep, bedroom air quality and quantity, temperature, etc. From birth to the last breath, we have always kept in touch with technology, 7 days a day, 24 hours a day throughout the year.

These conveniences are provided by the company on which the business is established. Technology serves us in many ways, which is a good thing. Modern technology and its development have made possible the vision of science fiction writers decades ago or a few years ago. It creates new business lines and good opportunities for technicians and companies willing to take advantage of this rapid development. Technology can help us in many ways, make our lives comfortable, and free up time to make life interesting and worth living. For companies, technology means new business opportunities or profitable ways to achieve business-supporting processes. It also means that companies must be able to consider cybersecurity issues, and this is where the biggest risk lies. According to the Nokia Group, in the computerized world in. President Risto Siilasmaa (Dahlgren 2016).

**2.7 The value of information**

In an organizational environment, information is the business enabler. Business processes (whether supported by information technology or not) generate and process data, which is converted into information and knowledge, which can be used to create value and promote the development of the organization and its processes (ISACA, 2012). Information management has been changing the way organizations promote business development and competition, and plays a key role in enhancing their strategic and competitive advantages (Saloojee et al., 2007). The organization makes explicit and implicit decisions about the needs and use of information.

These decisions are based on the estimated costs and benefits of information about its business structure and strategy (Feldman and March, 1981). Organizations are consumers, managers and providers of information. Their reputation in organizational intelligence is based on their ability to protect, analyze and retrieve information in a timely and effective manner (Feldman and March, 1981).

# 2.8 The CISO’s Role

CISO is responsible for the leadership of information and security systems. This official is mainly dedicated to meeting the information needs and promises claimed by the organization (Hooper and McKissak, 2016). Specifically, due to the immaturity of the name, according to the literature, the role of CISO is not very clear (Monzelo and Nunes, 2019). Other positions such as CEO and manager are defined because these positions are mature positions. In these positions, the company clarifies a variety of situations based on their responsibilities. The main responsibility of CISO is to explain how to formulate, manage and implement an organization's security plan, continuously evaluate the security plan, perform audit and risk management measures, and protect the company's intellectual assets.

CISO representatives or those responsible for information security indicate that leadership is needed to focus on information security needs and commitments in any organization (Peltier, 2013). The role may have other names, such as Director of Information Security, Information Security Manager or Information Security Officer, but the title is not as important as your responsibilities (Fitzgerald, 2007). Although the functions of the CEO and chief information officer (chief information officer) have been clearly defined due to the maturity of these roles, the definition of the role of the chief information security officer is still evolving (Fitzgerald, 2007). In the past, his responsibilities focused on defining technical security standards and policies. Nowadays, organizations are gradually realizing that cyber risks are directly related to their innovation and growth strategies (Goodyear et al., 2010). Nowadays, CISO is paying more and more attention in the definition of organizational information risk management strategy (Médice, 2013), and its main responsibilities are (SC Jobs, 2017):

* Formulate, manage and implement information security strategies;
* Continuously monitor and evaluate information security practices;
* Conduct information security audits and risk assessments;
* Lead, supervise and train your department and team;
* Make the organization comply with information security regulations;
* Formulate and implement a business continuity plan;
* Protect the intellectual property rights of the organization;
* Information security risk and strategy training and awareness of company employees;
* Manage information security budgets; and
* Report to the board of directors and be an active member of the senior management team.

CISO has an executive role in an organization and is responsible for establishing and maintaining an organization's information security vision, strategy and plan consistent with the overall organization strategy (Goodyear et al., 2010) (Peltier, 2013). Although it can be concluded that modern CISOs are essentially more in line with the administrative and senior management of the organization than in terms of technology (Cave, 2017), this is confirmed by research information from ISACA and RSA Conference and from managers and security experts, 63% of the respondents still report to the CIO, 14% report to the CEO, and only 8% report directly to the board of directors (ISACA, 2016).

# 2.9 Findings

According to the previous literatures following are some findings:

1. A positive impact of the regulatory changes on information security awareness in organizations and in different countries had been verified (Brown D 2017). The privacy requirements imposed by the GDPR is leading to a cultural change and there is hope that the implementation of the NIS directive will empower information security awareness (Ataya, G. 2017).
2. It was possible to identify a relationship between the CISO role in organizations and the awareness that exists for the subject of security within them. In organizations where there is less maturity for security issues, the person in charge of this area is typically under the IT department. In organizations where boards of directors are more aware of information security risks and their impact on business operations, organizational strategy, and reputation, the CISO has a greater proximity and independence with them (Bessen, James E 2017).
3. It had concluded that the CISO role and their mission in organizations may be directly related to the awareness that exists on the matter, and that information security is not only an organizational matter but also a social and cultural theme (Chaudhary, N et al. 2017).
4. Although it was not possible to conclude on the need for CISO to belong to the boards of directors, as defended by SC Jobs (2017), it was possible to understand the need for security matters to arrive to the top management without any filters and the need for a close relationship between the CISO and the boards of directors. The fact that it is not possible to draw a solid conclusion on the need for the head of information security to belong to the boards of directors could be directly related to the lack of maturity and culture for the subject

# 2.10 Summary

Information security is collectively regarded as a key and important factor for the success of any organization in the literature. In today's highly competitive era, information is known as the most important asset for competition in the market. In short, formulating IT management plans in companies is also a common practice in the business world, and it has been studied in depth in the literature. However, the field that requires extensive research belongs to the role of CISO in formulating and managing IT security plans for enterprises, which is still controversial in the literature. Therefore, current research explores the role of CISO and its supporters and opponents in formulating and managing company security plans. We investigate the role of CISO in managing risk, security operations, physical security and balancing enterprise and security objectives. The maintenance of information and security systems is the responsibility of CISO.

#

# Chapter 3: Research Methodology

# 3.1 Research Approach

The research method explains how the research will contribute to the existing theoretical framework. Specifically, the two main methods include deductive reasoning and inductive reasoning. The deductive method starts from the developed theory, and then progresses to the development of hypotheses and confirmation or denial of the theory. On the other hand, induction started with preliminary assumptions and led to the development of the theory (Taherdoost, 2016). In the current research proposed, when the results of the research will contribute to the theory of the role of CISO in the development and management of enterprise IT security plans, an induction method will be used.

# 3.2 Research Methods

There are two main research methods in the literature, such as quantitative methods and qualitative methods. Quantitative research is based on numerical data analyzed using statistical software (Kumar, 2019). In contrast, qualitative data consists of subjective information and result inference. In the current research, a hybrid method is used, in which quantitative and qualitative data are collected, the results are presented in a statistical manner, and the results are logically explained according to the methodology. Hence, by using the mixed methodology, it become easier for the researcher to extract the nature of relationship between the variables using the quantitative approach and also provides the reasoning for the certain relationship via the qualitative information.

# 3.3 Research Paradigm

According to Creswell (2009), the research paradigm refers to a certain basic principle that leads to concrete action. This is a broad generalization of something (Peffers, Tuunanen, Rothenberger, & Chatterjee, 2007). The paradigm is a way of observing the world, that is, these opinions or beliefs can affect the way in which researchers follow certain rules to conduct research, and can also affect the purpose of the research (Creswell, 2013; How to observe, investigate , understand, see or Comprehension of the world (Denzin and Lincoln, 2008) These beliefs enhance researchers' use of paradigms that can be qualitative, quantitative, or based on mixed methods (Creswell, 2013; Creswell and Clark, 2007).

Generally, in an independent study or a group of studies studying similar main phenomena (Leech, Dellinger, Brannagan, and Tanaka), a mixed-method study is responsible for collecting, analyzing, and interpreting qualitative and quantitative information. , 2010). Hybrid methods are used on the

basis of philosophical assumptions and research methods (Creswell & Clark, 2007), and the role of philosophical assumptions is to drive the scope of data collection and analysis, as well as to be carried out on the basis of independent investigation or separate investigation. Phenomenon uses a combination of qualitative and quantitative data collection methods. The main focus of hybrid research is to combine qualitative research with quantitative research, with sufficient understanding to solve research problems that cannot be solved with a single strategy (Creswell, 2013; Creswell and Clark, 2007). The dichotomy of the mixed method paradigm can be understood in the following flow diagram:

**

*Figure. 3.1.* The Methodological dichotomy (Creswell, 2013)

# 3.4 Rationale behind Selecting Mixed Method Approach

The research literature requires researchers to describe the reasons behind the choice of the hybrid research method (Creswell, 2013; Creswell & Clark, 2007). In this study, we will use the hybrid method described to study the basic logic behind (Fraenkel and Wallen, 2003), that is, the logic behind the hybrid method research is caused by the pattern of recognition (induction). Therefore, theoretical studies or hypothesis testing (inference) (Creswell, 2013; Creswell and Clark, 2007; Denzin and Lincoln, 2008; Fraenkel and Wallen, 2003; Leech et al., 2010) explain both (kidnapping).

# 3.5 Theoretical Frame of the Study

Hybrid method research will be conducted around a theoretical/philosophical structure that truly describes the general process of investigation, usually including a worldview or philosophy describing the philosophical basis and concept of knowledge, and a theoretical perspective to discuss the problem. The basic theory or main aspects of research. It is based on a methodological approach that questions the type of research researchers are using, and finally the data collection method used by the instrument content to collect information (L. Gay, Mills and Airasian, 2012). ; LR Gay, Mills and Airasian, 2011). Let us link our research based on the following structural basis.



*Figure. 3.2.* The Foundations of Social Research (Crotty, M. 1998)

# 3.6 A worldview or Philosophical Background

The research is usually based on some background worldview or philosophy (Creswell, 2013; Creswell & Clark, 2007). Basic philosophical assumptions include ontological basis (how to view reality), epistemological basis (how to obtain knowledge), axiological basis (how to view value), methodological basis (how to conduct research) and rhetorical basis (how to obtain knowledge). See language). The top four worldviews in a study are post-positivism, constructivism, participatory and pragmatism.



*Figure. 3.3.* Worldview of Philosophical Dimensions

For this study, the best paradigm that justifies mixed method research i.e. pragmatism ([Leech, et al., 2010](#_ENREF_143)), will be selected. The rationale behind selecting pragmatism is that:

* Recognize the use of qualitative and quantitative strategies in a study.
* The importance of research questions is more important than data collection methods and/or research paradigms.
* It gives the freedom to choose logical reasoning without any restrictive philosophy such as post-positivism or constructivism.
* The data collection strategy will be determined based on the research question rather than the type of research paradigm.

# 3.7 Methodological Approach

As mentioned earlier in this chapter, this research will be based on a hybrid method research paradigm that follows a methodology approach to hybrid method research design. According to research by Creswell (2013), there are two main hybrid method designs, namely basic method and advanced method. The former has three designs, namely convergence, explanatory sequence, and exploratory sequence design, while the latter also has three designs, namely, interventional, transformer, and multiphase design.

In this study, a convergent parallel design will be used to analyse the data and report the results. Convergent parallel design means that researchers perform quantitative and qualitative elements at the same stage of the research process, match the compensation method, analyse these two components separately, and then jointly explain the results (Creswell and Pablo-Clark, 2011).

To verify, the researchers aim to triangulate the method by directly comparing quantitative statistical results with qualitative results. During the research process, two data sets were obtained, analysed, and compared. The investigation process of this investigation is shown in the figure.



# 3.8 Research Design

This research is mainly based on quantitative data obtained through self-constructed questionnaires, but for triangulation, qualitative aspects are also included through interviews.

## 3.8.1 Triangulation Design

The term "triangulation" was originally coined by two quantitative psychology methodologists: Donald Campbell and Donald Fisk (1959) used it in their famous article on "multi-feature/multi-method matrix" Terminology to provide what they think is an alternative. The "simplified operation" of many psychologists. Both authors advocate the use of different measurement tools to capture psychological characteristics, and use the statistical correlation between the results of different measurement operations to determine the effectiveness of the "convergence" and "differentiation" of this structure. This idea was later extended to a combination of various data and data collection methods to compensate for their respective effectiveness limitations (Webb et al., 1966). The qualitative social researcher Norman Denzin adopted this idea in his "The Research Act" (The Research Act) in 1977 and distinguished different forms of triangulation (that is, theory,

data, method and research triangulation) To extend this concept. The combination of qualitative and quantitative methods represents a possible type of method triangulation. Methodological

triangulation will involve "a complex process, comparing each method with each other to maximize the effectiveness of field work" (Denzin, 1977).

## 3.8.2 Rationale behind using Triangulation

The concept of methodological triangulation can be viewed in two different ways: by using different methods to verify the results, or as a combination of methods and/or data, with the purpose of describing a field or research topic more completely and using different Complementary results are better explained (Erzberger & Kelle, 2003; Kelle & Erzberger, 2004).



If you examine the example of method triangulation from research practice, he will find that all three readings of the triangulation metaphor are suitable for describing specific situations where qualitative and quantitative methods are combined:

1. Triangulation to test the validity of the research results (quantitative or qualitative)
2. The purpose of triangulation is to better understand through supplementary discovery, this result can also exist alone or placed in a wider range.
3. Triangulation is a way to generate a complete result by discovering two parts that cannot be maintained by itself.

In this study, given that the goal is to investigate the role of CISO in the design and management of integrated enterprise IT security plans, triangulation will be used to supplement the results of quantitative and qualitative data.

# 3.9 Data Sources and Collection Technique

Researchers are using primary and secondary data sources to collect useful data for research. Specifically, the primary data is collected directly from the interviewees, while the secondary data is collected from sources that publish information and can be used for research (Synder, 2019). In the proposed study, main data will be collected for quantitative and qualitative assessment of the role of CISO in the development and management of the company’s IT security plan. Qualitative data will be collected through semi-structured interviews, while quantitative data will be collected

through questionnaire surveys. In order to collect data, the CISO will be contacted via email, and an online questionnaire will also be developed, which will contain unresolved questions that the CISO will answer. Therefore, a link to the questionnaire will be shared in an email requesting data for academic purposes and ensuring that your data will be kept confidential. In order to collect data through interviews, I will personally visit some organizations, agree to accept interviews, and make appointments based on CISO’s convenient sources, such as face-to-face meetings or video calls. In the process of visiting CISO, I have some personal links in the organization to help me conduct interviews. However, for investigation purposes, I will provide my university recommendation letter to different organizations through a permit letter to seek help from different organizations. In addition, the secondary data will also be used in the form of a literature review, where the published literature will be used to establish the theoretical basis for the research.

# 3.10 Sampling

In the proposed research, non-probabilistic sampling will be applied together with convenient sampling techniques. Basically, the reason for choosing a suitable sample is based on the fact that it covers the limitations of researchers and helps to obtain suitable data (Mohajan, 2018). The specific sample includes CISOs from 30 German organizations. Specifically, all 30 questionnaires will be interviewed to complete the questionnaire, and 5 CISOs who are willing to obtain qualitative data will also be interviewed.

# 3.11 Data Analysis Techniques

To perform quantitative data analysis, descriptive statistics will be applied together with the frequency table and bar graph in SPSS software. This will help to play the role of CISO in the development and management of security IT plans, as well as the factors that help or hinder the

effective performance of CISO responsibilities. In addition, subject analysis will be conducted based on the principle of exploring the role of CISO in the organization to analyze qualitative data.

# 3.12 Research Limitations

According to the way the data is collected and analyzed, research has certain limitations. Specifically, in the proposed research, the main constraints include the minimum resources available for conducting the research in terms of time and finance due to the selection of a limited number of respondents. In the future, because the information system of any organization is a sensitive subject, the target interviewees are also restricted, so the interviewee may be reluctant to provide feedback on the topic.

#

# 3.13 Methods of Data Collection

In the previous literature, several tools for the qualitative and quantitative parts of the social sciences and behavioural sciences have been identified (Tashakkori and Teddlie, 2008; Creswell, 2008; Creswell and Plano Clark, 2007; 2011; Bryman, 2008). These studies show that all types of interviews, observations, checklists and documents (text/pictures) can be used for qualitative data collection, while all types of survey tools, performance tests and experimental tests can also be used for quantitative data. The data collection techniques in this chapter will discuss the instruments used in this study.

This research will follow a hybrid approach. For the collection of quantitative data, questionnaires will be used as a tool, and for the collection of qualitative data, interviews will be conducted with 5 CISOs.

# 3.14 Instruments of the Study

Two instruments will be developed for this research. A questionnaire will be developed for the CISO and interviews will be conducted with 5 willing CISOs.

***Validity of the Quantitative Instrument***

The validity of the questionnaire will be determined and improved through experts’ opinion.

***Reliability of the Quantitative Instrument***

Pilot tests will be performed on 10 CISOs not included in the sample to determine the reliability of the instrument. Cronbach's Alpha test will be used to find the alpha value.

**Qualitative Instrument**

***Semi-Structured Interviews--*** In qualitative research, interviews and other techniques are usually used to explore related concepts that depend on certain people, background, time, and circumstances (Taylor, 2012). Interviews are referred to as communication or dialogue between two people to extract their respective information (Cohen, Manion and Morrison, 2007). Types can be informal or formal, structured, semi-structured or unstructured. In qualitative research, semi-structured interviews are considered to better mark the conscious experience of participants living under specific phenomena, and are enclosed in parentheses (Manen, 1990; Moustakas, 1994; Marshall & Rossman, 2010).

In this study, semi-structured interviews will be used as one of the data collection sources. The strongest reason to use it is that these types of interviews are also called "purposeful conversations" (Anyolo, 2015). These are important for discovering basic information about selected participants (Mweti and Van Wyk, 2005). These methods are very useful in a time-consuming way, and the advantages can be seen in this technique, because the researchers can discover things that cannot be achieved with any other method (enclosed in parentheses). The time is not limited, and it may take up to 2 hours or more (Yin, 2012). Another fundamental reason is the large amount of data that can be provided by semi-structured interviews (Yin, 2012), which is also the basic feature of our qualitative stage and participant selection criteria.

**Experts’ Opinions**

After establishing the access agreement, the researchers adopted expert opinions on the language, content and environment of the instrument. For these two local experts, they will be contacted. Experts suggest some modifications to these three tools and require a preliminary collection of a participant from each group so that they can be refined according to the situation faced by the researchers. The fact is that since both protocols will only ask the main questions, which are semi-

structured questions, after each session, they will be streamlined for the next interview. The method will be the same, that is, indicate in parentheses which conscious experience they live in.

# 3.15 Data Collection

## 3.15.1 Quantitative Data Collection

The data will be collected by the researcher personally by visiting the organization in person or sending it via email. The researchers obtained the consent of the university. Investigators must ensure that they stay at the distribution site for a period of time to ensure that each participant understands the content of the questionnaire and how to fill it out. They will get an estimated 3 days to return the complete questionnaire. After each collection, the researcher will provide an identification number for each instrument received so that it can be tracked as it enters the MS. Excel or SPSS spreadsheet.

## 3.15.2 Qualitative Data Collection

After completing the program, the researcher will contact each participant/selected member by phone, and after determining the willingness to participate, the interview time will be determined according to its availability and feasibility. Each interview begins with a brief introduction to the interviewer, the interviewee and the purpose of the research. The researchers clearly talked about ethical considerations in establishing a trust relationship between the two. Each conversation took nearly 30-35 minutes of conversation time and recorded it on the Android phone voice recorder. After each course, interviews will be transcribed immediately to find new life experiences and novel topics. This is done to establish the saturation between interview sessions, that is, each new information, idea, concept or topic will also be asked to the previous interview participants. In this way, the saturation point between the information can be Up. The interview is here.

# 3.16 Data Analysis

**Quantitative Data Analysis**

Descriptive analysis will extract the range of practice with the help of mean and standard deviation values, while using t-tests to determine demographic differences. The demographic information of the participants will also be determined based on the percentage of participants and a cross-tabulation.

**Qualitative Data Analysis**

After completing all interviews, they will be eligible to be transcribed. In this study, we used the data interpretation process discussed by Hycner (1999). He used the word "analysis" in the study to warn the researchers because it meant to be divided into several parts. The completeness of experience/phenomenon (Hycner, 1999) proposes the following steps to interpret the data:

1. Bracketing and reducing experience/phenomenon
2. ii. The entity that portrays meaning
3. iii. Group the important entities that make up the theme
4. iv. Summarize each interview session and provide necessary instructions
5. v. Draw similar and different topics from each interview session and generate a comprehensive summary.

***Bracketing and Reducing the Experience/Phenomenon-***  It is a method of marking, highlighting, pointing out, emphasizing, or surrounding/conscious/deliberate experiences under the current phenomenon described by the participant. This is not to reduce the phenomenon, but to limit the bias of researchers based on their own assumptions and guide the researchers to derive the correct meaning from the text (Creswell, 2013; Moustakas, 1994; Marshall & Rossman, 2010; ML. etc. Hycner) ,Year 1999). Therefore, in this study, the researchers copied the records immediately after

conducting each interview, and began to add the real experience mentioned in that interview in parentheses. She will add parentheses after each experience based on related research questions.

***Outlining Meaningful Entities--***  This is a crucial stage in the sense that the researcher must transform the statement enclosed in square brackets into meaningful entities/components to extract the statement that the researcher clarified (Creswell 2013; Hycner, 1999). It is done by observing the number of times the event is mentioned and how the event is handled, that is, the time sequence and depth of the event/experience (Hycner, 1999). Therefore, this research will be conducted on the basis of the information needed to answer the research questions.

***Grouping Meaningful Entities forming Themes-***- The topic group usually consists of important entities (Creswell, 2013; Moustakas, 1994), and researchers must recognize the important and necessary topics to be discussed (Sadala and Adorno, 2001), because in our case, each question involves Subject survey. To answer.

***Summarizing every Interview Session-*** This is done to fully understand what is stated in the information provided in the topic (Hycner, 1999). Since the purpose of phenomenological analysis is to explore the depth of life of the subject under this phenomenon, each individual of the phenomenon may have different ways of interpreting and interpreting things. Therefore, it is necessary to keep things integrated in order to understand all the "depth" of the subject's inner world (Ellenberger, 1958; Mycner, 1999). In our research, we also try to maintain integrity so that we can correctly give answers to research questions.

***Similar and Dissimilar themes making a compound Summary--*** Once all the above-mentioned work is completed in each interview, the researcher must study the commonality and uniqueness between them. This is done by not grouping topics that still have differences (Hycner, 1999). Therefore, first summarize the common themes and give a detailed description, and then state their uniqueness or novelty, and explain why they are so important, so that researchers can make suggestions. For this research, Chapter 4 of this paper provides detailed explanations. These explanations rank similar and different topics in interviews with participants.

# 3.17 Motivation

Technology has become a vital success factor in people's lives in all fields, multinational companies and countries/regions. It can make the subject reach the height of success, and it can also make him fall into a serious crisis, which depends on its effective use and security guarantee

against network attacks. In this regard, it is interesting to explore how organizations manage their IT security.

How CISO designs and manages plans. Finally, the proposed research looks for ways for companies to deal with new technologies that make it easier for cyber ghosts to invade the company’s information systems. All these general questions motivate researchers to choose topics for research purposes.

# Chapter 4: Findings and Analysis

# 4.1 Overview

The present section is consisted of explaining the findings of the study which are extracted through the collection of the data. Mainly, the current research study has gathered two types of data such as the quantitative data using the questionnaire and qualitative data using the interviews. Hence, the findings of the study are also distributed into two major sub-sections such as the statistical findings for the quantitative data are presented first and then the thematic analysis for the qualitative data is presented. Afterwards, the study also provides the analysis of the findings also in light of the existing literature to identify that either the findings are backed by the literature or these are unique in nature.

# 4.2 Statistical Findings

The questionnaires are developed in order to gather the data from the CISO. Mainly, three sections are defined for the study variables in the questionnaire where the first one asks about the responsibilities of the CISOs while the second and third is associated with the enablers and hinderance factors which are faced by the CISOs for meeting the responsibilities.

*Table 4.1: Responses to the Questions*

|  |  |
| --- | --- |
| **Question** | **Responses** |
|  | *Yes* | *No* | *Rarely* |
| **Responsibilities as CISO:** |  |  |  |
| Strategic security management | 14 | 3 | 3 |
| Risk management in security plans | 17 | 1 | 2 |
| Providing training and awareness regarding security plans to the employees | 18 |  | 2 |
| Compliance of regulations and standards | 11 | 3 | 6 |
| Maintaining high data security | 10 | 4 | 6 |
| Procuring the technology by reviewing different security aspects | 17 | 1 | 2 |
| Develop the list of interested parties related to information security  | 14 | 1 | 5 |
| Teach employees how to perform risk assessment | 15 | 2 | 3 |
| Coordinate all efforts related to personal data protection | 8 | 11 |  |
| Propose the selection and deadline for safeguards implementation | 9 | 5 | 6 |
| **Enablers in performing responsibilities:** |  |  |  |
| Interpersonal support by employees | 17 | 2 | 1 |
| Cooperation and teamwork | 17 |  | 3 |
| Collaboration by all departments | 19 | 1 |  |
| Conflict resolution by regulations | 15 | 3 | 2 |
| Advanced technologies | 17 | 3 |  |
| **Hindrances in performing responsibilities:** |  |  |  |
| Hackers attacks by competitors via spy marketing to access the company’s data | 20 |  |  |
| Higher costs of advanced technologies | 18 | 1 | 1 |
| Centralized structure of organization which creates issues in taking timely decisions | 17 | 3 |  |
| Unfavorable behavior by employees | 20 |  |  |
| Lack of coordination among different departments of the organization | 17 | 2 | 1 |

It is analyzed from the findings of the study that the responsibilities of CISO are consisted of multiple aspects. Mainly, the surveyed CISOs have accepted mostly that the strategic security management is included in their job role and responsibility. 14 CISOs said that these are the roles included in their jobs while 3 said that they are not responsible for the security management and remaining three opted for the option of rarely doing this job. Secondly, the risk management in security plan is also included in the job description of most of the respondents. Besides the development of the risk security plans, the CISOs also plan and provide the training to the workers for the security management. However, many CISOs explain that they are not responsible for ensuring the compliance with the rules and regulations. The maintenance of the data security is assigned to most of the CISOs to enhance the credibility of the data. Besides that, the procurement of security, development of the list for the parties’ interest in the security of the data, teaching employees regarding the personal of the security plans, coordinating the efforts for the personal data protection and safeguard implementations are included in the jobs of the CISOs.

It is extracted from the findings that there are multiple factors which are facilitating the CISOs to perform their roles and duties. These factors include the collaboration by all departments to be at the most significant level as it is the factor opted by almost every CISO that it enables them to perform their task. Besides that, the supporting factors include interpersonal support by the employees, cooperation with team work, advanced technologies and conflict resolution by regulations. Hence, it is extracted that the CISOs are facilitated by the different factors to perform

their roles and responsibilities. However, there are also some hurdles identified via the survey which includes the spy marketing where the hacker’s attacks are considered the significant hurdle threatening the security of the system. Moreover, the unfavorable behavior by the employees is also considered as the most significant hurdle by all the CISOs which have participated in the survey. Besides that, the higher costs of the advanced technologies create the hurdles for the CISOs to attain the latest versions of the software and the hardware to get to the desired level of the information security. Moving ahead, the centralized structure and lack of coordination by the employees of the organizations all are perceived as the hurdles to perform the duties of the CISOs in the companies.

# 4.3 Thematic Analysis

The interviews are conducted with five CISOs and the outcomes are analyzed using the thematic analysis. The thematic analysis is consisted of the questions, common responses, focused coding and developing the themes out of the responses. These themes are then discussed in the discussion section along with the views of other researchers.

*Table 4.2: Thematic Analysis of Interviews*

|  |  |  |  |
| --- | --- | --- | --- |
| **Questions** | **Responses** | **Focused Coding** | **Themes** |
| What are your core responsibilities as CISO? | We are here to perform different security related operations and its management by mitigating the risks and enhancing the governance of the security management | Security operation managing, cyber risk management, program management, governance  | CISOs are responsible for the information security of business |
| Do you assist in marketing intelligence of the business? | The information security provides the risk-free plans to the business, hence it does facilitate the marketing but as a CISO I have never assisted the marketing intelligence  | No |  |
| What are the common factors which help you in performing your responsibilities? | The cooperation of the workers and the incorporation of the new technologies are very effective if these are intended to behave positively  | Workers behavior and advanced technologies |  |
| How advancements in technology are affecting IT security plans? (Positively: by enhancing the strength and negatively: by equipping the hackers) | Security operations management is totally dependent upon the advanced technologies so with the help of these technologies, the security of the information become much easier and effective  | Positively  |  |
| Do you follow triage process in your IT security plans? | Yes, we try to deal the issues on the priority bases as per their significance | Yes |  |
| What are the common threats you face in your IT security plan? | the external attacks are the most threatened factor where the information as well as the system is at the risk  | External attacks |  |
| What are the factors causing issues for you to perform your duties? | Higher costs of the advanced technologies, lack of cooperation by the employees and lack of freedom to take the timely and effective decisions | Higher costs, adverse behavior and central structure  |  |
| How you would conclude the role of CISO in designing and managing the IT security plan of an organization? | CISOs are responsible for keeping their organization’s digital and information assets safe and secure. | Securing digital assets |  |

# 4.4 Discussion

This research indicates that CISOs embodied in this study consider different roles as highly significant. However, pace at which each of these duties varies according to the needs of the state agency, CISOs are attempting to address importance of information security safety. Although information security directors have replied to the questionnaire, more than half of the respondents in this study did explicitly reflect the CISO word. It is important to point out that since technology is evolving rapidly, so are the everyday tasks of CISOs. results showed that CISOs not only take on technological responsibility, but are having deep concern about details.

Nevertheless, each survey item was analyzed individually and was used to understand the significance of each responsibility. In order to describe the significant responsibilities of CISOs in state agencies in Texas, survey questions were developed that addressed five categories each. In table 4.1, a summary of the results of the survey is presented.

As a significant managerial obligation, an overwhelming number of respondents supported risk control, incident response, budget and telecommunication. This shows that among respondents, there is a notion that recognizes management roles as very or extremely significant. The findings of the study, however, contrast with recent literature that involves the creation of software as part of CISO responsibilities. In their current position, for example, 66 percent of respondents suggested that they do not build software. Unlike technological duties, forty-four percent of respondents preferred the acquisition of the device as a very or highly significant duty. Likewise, thirty percent of respondents said copyrights were mildly or moderately significant. The results of the survey showed many other important findings. Respondents thought that knowledge of the faculty and technical consistency were very or highly important obligations for career growth. Fifty-six respondents, unlike certifications, thought such transparency was marginally or moderately significant. One of the most contentious duties are related to information security since they deal with sensitive data. Eighty-nine percent of respondents believed that it was very or extremely necessary for data protection. Seventy percent of respondents said it was very or extremely necessary for network security. Similarly, 67% of respondents also said access controls were very or extremely necessary.

The IT security of a company has historically come under the IT security manager, or the risk manager. Nevertheless, it seemed that the position and its duties were an offshoot of IT. Usually, it was put in the IT department, reporting to the CISO or someone with a comparable role. While such an arrangement made sense, the downside was that IT protection was diluted not only in terms of attention or reporting, but because it is largely invisible in an organization's everyday activities, in terms of budget allocation, in the multitude of other aspects for which IT is responsible. Consequently, the reporting to the executive/board was often diluted and, in terms of its image, protection appeared to disappear into the background unless there was a significant breach. The increased general knowledge of the significant potential risk of security breaches has prompted

organizations that are especially security conscious, such as government agencies and banks, to create a place to be in charge of their protection at a higher level than the IT security manager. Thus, the CISO position came into being. The CISO is a position at the strategic level, responsible for ensuring that information assets and IT systems are safe and secure and that such security is in line with the organization's strategic strategy. Where to position the CISO was the issue. If put under the CIO or Head of IT, the CISO might benefit in many respects from the assistance of the CIO rather than having to fight for financial resources with the CIO, for example. This form of design gives the company the potential for greater efficiencies and enhanced service. However, if the need were to arise, it would be hard for the CISO to blow the whistle on the IT department. Many organizations that are very focused on the integrity of their data, particularly in the government sector, seek to maintain the independence of the CISO and place the CISO at a level equal to the CIO outside the IT department. This offers freedom, but with regard to the responsibility of the CISO and dependency on its IT base, it may also become problematic. A hybrid, with a break between operations and the more strategic stage, is a third configuration. An IT security manager will operate under the IT umbrella in this case and be in charge of technical operations. The CISO will work independently and be accountable for the security strategic aspects. Organizations that have formed independent CISO roles typically have the CISO reporting directly to the CEO, given the increased knowledge of IT security/ cybersecurity and the appreciation of the value of safeguarding their information assets. This is the case in many departments of government, where the need for scrupulous independence and custody of information is very much the priority. Thus, governments establish an autonomous CISO role, while organizations, such as very IT-dependent banks, allow the CISO to fall under the CIO. Usually, small organizations don't have a CISO role and the CIO manages security. Depending on their market emphasis and scale, companies thus adopt every one of these organizational configurations. Typically, the job descriptions of CISO roles have been taken from three sources: the incumbent, a role description used as a reference from a similar company, or an industry standard. A mixture of two or three sources is sometimes utilized. The first source is more popular than is generally accepted. The CISO is most often someone who has risen through the IT ranks, first being a manager of IT security and then the CISO. These CISOs have good experience and

awareness of IT. Instead, they may have come up through the ranks of risk management, in which case their objective would not necessarily be as technical.

The invisibility of protection success is one of the main challenges that CISOs face. Usually, performance goes unheralded, while violations can attract tremendous publicity. In general, success is not known to be a product of proactivity. If it is celebrated, it is in reaction to a satisfactory response to a violation that has already happened, where the harm is reduced and the continuity of business is not too interrupted. More often than not, if the reaction is unsuccessful, the response is to blame the security department instead of celebrating every obstacle faced or assault thwarted. While boards worldwide are concerned about their protection, it is difficult for board members to understand the spectrum of such activities and judge if what is being done is appropriate by the invisibility of much of the positive activity ensuring security. Plus, security performance monitoring is frequently swamped by any number of more pressing problems. Private companies, for example, will be more concerned with the welfare of creditors, share prices, and income before a security attack hits the company. As a communicator, the ability to understand what is important to both business and technical audiences demands performance in the CISO role. It is doubtful that the challenges encountered by executive team members are the same as those within the company who are designing and administering security controls. The task of the CISO, having understood the expectations of all stakeholders, is to clarify security principles in terms that can be understood within the C-suite (e.g. through the use of analogy) and to inform the security team about the business factors that guide the security investment emphasis. In his paper, Stephen Boyer, co-founder and CTO of BitSight Technologies. In no way should any member of the board have to behave as a security expert. But cyber risks are a big part of managing risk in an organization in today's world. Therefore, board members ought to make what they see as important and how to launch these discussions known. It is important for the CISO to ensure that the security team understands what information is needed, how conversations should be framed, and the degree of abstraction required by decision makers, serving as a conduit of security information to the executive and, eventually, the board. Otherwise, the CISO will have discussions with the organization that do not resolve the most important issues. The CISO will also collaborate with risk practitioners to define the most important security threats, based on an understanding of the business strategy of the company. In relation to business partners and suppliers, the CISO also

needs to consider risk. To get into a targeted organization, vendors may be used as a backdoor. A growing emphasis of security managers is third-party assurance as companies become increasingly linked. Indicators of security risk assist CISOs in determining risk exposure. Such metrics could include the number of monthly attempts from established sources of cyber espionage to enter the corporate network, attempted intellectual property theft, or quarterly revenue losses associated with instances of customer data leakage. In order to communicate to the board, these primary risk indicators are critical because they help to demonstrate the strengths and limitations of the general security posture of an organization. Risk measures such as these can be used to tell board members and fellow managers a story. Stories will help business managers understand what particular threats the company is targeting, what the attacks look like, and what they can do to help prevent a breach.

Having defined the risk background and developed security stories, the CISO's function is then to effectively communicate the organization's safety performance and capability. A robust collection of metrics based on ISO 27001 or other security frameworks also underpins executive safety assurance and performance metrics reports, risk and compliance reviews, and ROI interventions. The problem with such detailed security reporting is that it is typically understood that it is extremely difficult to communicate security information, especially with non-technical, disinterested, or time-constrained C-suite executives. The general tendency for security briefings to take place less regularly than the monthly or quarterly briefings for other business disciplines such as finance, HR, or development does not help solve this problem. An industry-sponsored survey on the state of risk-based protection found that most senior executives only ask to hear from their CISOs when breaches have occurred or when a need-to-inform crisis level is struck by other security crises.

Given the CISO's duties, some important developments were expressed in the criteria for the applicant organizations sought. Considerable experience was required: typically, at least 10 years in IT, 5-10 years in defense, and 5-10 years at risk, in which a senior management/leadership position should have been for at least five years. Just one or two organizations, however, required proof of significant achievements in those particular fields. The CISO should also be knowledgeable about the market climate, although this was not stated in all advertisements.

Knowledge of that particular industry was needed, especially for organizations in the health sector. As far as education is concerned, a degree in computer science or related fields such as IT is commonly necessary. A master's degree was sometimes suggested, suggesting either more specialization or, rarely, more of a business emphasis as reflected in an MBA. However, there was typically a need for an overwhelming list of industry credentials, such as CISSP, CSSLP, CCFP, CISA, and CISM. For example, one job required experience with scanning vulnerability tools, scanning vulnerability tools for web applications, static analysis tools, and current security certifications such as CISSP, CSSLP, CCFP, GSSP-JAVA, and GSSP-NET. Furthermore, occasionally experience of ethical hacking tools was included. Knowledge of specific systems, including auditing systems such as the ISO/IEC 2700 suite, structures such as CoBIT, COSO, and ITL, and international standards and regulations such as those supported by NIST, SOX, and HIPAA have generally been required. Although some advertising concentrated on strong technical skills, such as Java programming experience and cryptography expertise, other jobs sought a CISO that was proficient in the use of PCs and Microsoft Windows. This variety is shocking, particularly for anyone heading up a department of information security. Sometimes, familiarity with Microsoft Windows is believed to be readable in a similar way. On the other hand, it is understandable to concentrate overwhelmingly on professional skills and expertise, but in many cases, it was in violation of the need for corporate experience and the ability to interact with the rest of the company and the board. Some organizations were searching for a CISO who had outstanding communication skills, such as verbal, written, or public speaking. However, others (although in the minority) took things further, preferring someone with exceptional analytical abilities, an uncommon ability to move quickly to resolution, and an ability to provide versatile security solutions. One corporation was searching for someone with a powerful executive presence. A couple of ads sought a CISO with solid business and information security ethics and understanding, as well as an expert degree of personal honesty. The latter criteria are interesting because, of all people, a high degree of personal integrity should be held by someone in charge of protection. However, often it is important to state the obvious and, as shown by the examples in the introduction, it is always those entrusted with highly sensitive information that leak it. Overall, there seems to be a clear technical and security emphasis on both the role/job descriptions and the applicant requirements and that each of them evidenced the comprehensive technical/security skills as being of primary importance, while containing some elements of business knowledge and understanding. In many of the long lists in the job descriptions, given the combination of strategic and operational tasks, the perception is generated that, while they know CISOs can play a strategic role in their organization, organizations delegate the role to many operational tasks.

# References

Allianz (2016). *Allianz Risk Barometer - Top Business Risks 2016*. Consulted in 9th October

 2017.Availablein <http://www.agcs.allianz.com/assets/PDFs/Reports/AllianzRiskBarometer2016.pdf>

Anton, M. T., & Jones, D. J. (2017). Adoption of technology‐enhanced treatments: conceptual and practical considerations. *Clinical Psychology: Science and Practice*, *24*(3), 223-240.

Approach (2017). *Why do you need a CISO?*. Consulted in 18th March 2018. Available in

 <https://www.approach.be/en/images/gdpr_-_why_you_need_a_ciso-short.pdf>.

Allianz (2016). *Allianz Risk Barometer - Top Business Risks 2016*. Consulted in 9th

 October 2017.

 <http://www.agcs.allianz.com/assets/PDFs/Reports/AllianzRiskBarometer2016.pdf>.

Ataya, G. (2017). *Can a CISO act as a DPO?*. Consulted in 18th March 2018. Available in

 <https://www.linkedin.com/pulse/can-ciso-act-dpo-georges-ataya>.

Avila, O., & Garcés, K. (2017). Change management support to preserve Business–Information technology alignment. *Journal of Computer Information Systems*, *57*(3), 218-228.

Bessen, James E., Industry Concentration and Information Technology (December 1,

 2017). Boston Univ. School of Law, Law and Economics Research Paper No. 17-

 41, Available at SSRN: [https://ssrn.com/abstract=3044730](https://ssrn.com/abstract%3D3044730)

Beriev, I. R., Daudov, I. M., Tazbieva, Z. A., Goltakov, B. K., Malsagova, R. S., & Dadashova, A. S. (2019, March). Role and Significance of Information Technologies in the System of Human Resources Management. In *VIII Science and Technology Conference “Contemporary Issues of Geology, Geophysics and Geo-ecology of the North Caucasus”(CIGGG 2018)*. Atlantis Press

Bowen, P., Hash, J., & Wilson, M. (2007). Information security handbook: a guide for

 managers. In *NIST SPECIAL PUBLICATION 800-100, NATIONAL INSTITUTE*

 *OF STANDARDS AND TECHNOLOGY*.

Brown, D. (2017). *Is New Regulation a Threat or an Opportunity for Security Strategy?*

 Consulted in 18th March 2018. Available in

 [https://www.fireeye.com/blog/executive-perspective/2017/05/new-regulation- security-strategy.html](https://www.fireeye.com/blog/executive-perspective/2017/05/new-regulation-%20%20%20%20%20%20%20%20%20%20%20%20security-strategy.html).

Cave, K. (2017). *Does the CISO role need to be formalised?*. Consulted in 18th March

 2018. Available in

 <https://www.nacdonline.org/AboutUs/NACDInTheNews.cfm?ItemNumber=40736>.

Catarino, T. M., Vasconcelos, A., & da Silva, M. M. (2016). *The Role of the Chief Information Security Officer.* IST, Portuga.

Cupiał, M., Szeląg-Sikora, A., Sikora, J., Rorat, J., & Niemiec, M. (2017). The use of IT

 tools for knowledge management in companies, No. 20.

Chaudhary, Nitin; Miller, Paul A; Smith, Benjamin (2017): Modelling past, present and

 future peatland carbon accumulation across the pan-Arctic. PANGAEA,

 <https://doi.org/10.1594/PANGAEA.880524>.

Chaudhary, N et al. (2017): Modelling past, present and future peatland carbon

accumulation across the pan-Arctic. Biogeosciences Discussions,1-45 <https://doi.org/10.5194/bg-2017-34>.

Carr, N. G. (2003). IT doesn't matter. *Educause Review*, *38*, 24-38.

Cadete, G. (2015). Using Enterprise Architecture for COBIT 5 Process Assessment and

 Process Improvement. *IST, Portugal*.

Catarino, T. M., Vasconcelos, A., & da Silva, M. M. (2016). The Role of the Chief

 Information Security Officer. *IST, Portugal*.

da Silva, M. B. D., dos Santos, A. M., dos Santos Soares, M., do Nascimento, R. P. C., & Nunes, I. D. (2018). A survey on adoption good practices for ICT governance at enhanced organizations. In *Information Technology-New Generations* (pp. 483-490). Springer, Cham.

***Danchev 2003***, ***Greene 2014***.) Page 27. 22. 5.2 Information Security Frameworks and

 Tools.

Doughty, K. (2003). Implementing enterprise security: a case study. *Computers & Security,*

 *22(2)*, 99-114.

Fitzgerald, T. (2007). Clarifying the roles of information security: 13 questions the CEO,

 CIO, and CISO must ask each other. *Information Systems Security, 16*(5)*,* 257-263.

Feldman, M. S., & March, J. G. (1981). Information in organizations as signal and symbol.

 *Administrative science quarterly, 26(2),* 171-186.

Goodyear, M., Goerdel, H., Portillo, S., & Williams, L. (2010). Cybersecurity management

 in the states: The emerging role of chief information security officers. *Available*

 *at SSRN 2187412*.

Gulmira, A. (2019). THE ESSENCE AND SIGNIFICANCE OF INFORMATION TECHNOLOGY IN MANAGING THE COSTS. *Бюллетень науки и практики*, *5*(3).

Homeland Security Today (2017). *Oversight Transparency of Cyber Risks at Publicly Traded*

 *Companies Addressed in New Bill*. Consulted in 18th March 2018. Available in

 <https://www.hstoday.us/channels/global/oversight-transparency-of-cyber-risks-at->

 publicly-traded-companies-addressed-in-new-bill

Hooper, V., & McKissack, J. (2016). The emerging role of the CISO. *Business Horizons*, *59*(6), 585-591.

ISACA. (2016). *State of Cibersecurity Implications for 2016: An ISACA and RSA*

 *Conference Survey*. Consulted in 18th March 2018. Available in

 http://www.isaca.org/cyber/Documents/state-of-cybersecurity\_res\_eng\_0316.pdf

ISACA. (2012). *COBIT 5: Modelo Corporativo para Governança e Gestão de TI da*

 *Organização*. Rolling Meadows: ISACA.

International Organization for Standardization. (2017). *ISO/IEC 27001: 201*4: *Information*

 *security management systems - Overview and vocabulary*. International

 Organization for Standardization.

Josi, M. (2016). *What does the new EU Network Information Security Directive imply?*

 Consulted in 18th March 2018. Available in <https://www.cyan.network/news/what->

 does-the-new-eu-information-security-directive-implies.

Kumar, R. (2019). *Research methodology: A step-by-step guide for beginners*. Sage Publications Limited.

Luftman, J., Lyytinen, K., & Zvi, T. B. (2017). Enhancing the measurement of information technology (IT) business alignment and its influence on company performance. *Journal of Information Technology*, *32*(1), 26-46.

Mohajan, H. K. (2018). Qualitative research methodology in social sciences and related subjects. *Journal of Economic Development, Environment and People*, *7*(1), 23-48.

*Monzelo, Nunes / The Role of the CISO in Organizations Conferência da Associação*

 *Portuguesa de Sistemas de Informação (CAPSI’2019).*

Monzelo, P., & Nunes, S. (2019). The Role of the Chief Information Security Officer (CISO) in Organizations.

Médice, R. (2013). *O Papel do Security Officer (Agente de Segurança)*. Consulted in 18th

 March 2018. Available in <https://www.profissionaisti.com.br/2013/07/o-papel->

 do-security-officer-agente-de-seguranca/

Morimoto, S. (2018). Application of COBIT to security management in information

 systems development. In *2009 Fourth International Conference on Frontier of*

 *Computer Science and Technology* (pp. 625-630). IEEE.

MSB. (2017c). Frågor och svar om it- incidentrapportering.*Cert.se.*Available at:

 https://www.cert.se/it -incidentrapportering/fragor-och-svar/ [2018 -05-21].

MSB. (2016). Obligatorisk it-incidentrapportering. *MSB.se.* Available at:

 <https://www.msb.se/sv/Forebyggande/Informationssakerhet/It-incidentrapportering/>

 [2018-05-17].

National Cyber Security Center (2017). *Networks and Information Systems (NIS) Directive:*

 *Security objectives and principles*. National Cyber Security Center

Olijnyk, N. V. (2015). A quantitative examination of the intellectual profile and evolution

 of information security from 1965 to 2015. *Scientometrics, 105(2)*, 883-904.

Peltier, T. R. (2013). *Information security fundamentals*. CRC press.

Posthumus, S., & Von Solms, R. (2015). A framework for the governance of information

 security. *Computers & security*, *23*(8), 638-646.

Rollenhagen, C. & Wahlström, B. (2013). *Ledning av säkerhetskritiska organisationer*

Lund: Studentlitteratur.

Roland, N. (2017). *Would my CISO be my DPO? Information Technology Privacy.* Consulted

 in 18th March 2018. Available in <https://commyounity1.wordpress.com/2017/06/23/would-my-ciso-be-my-dpo>

Ross, A. (2017). *What is the Cybersecurity Disclosure Act of 2017?*. Consulted in 18th March

 2018. Available in https://baydynamics.com/blog/video-cybersecurity-disclosure-act-2017

Sajko, M., Hadjina, N., & Sedinić, I. (2011). Information security governance and how to

 accomplish it. *MIPRO, 2011 Proceedings of the 34th International Convention*. IEEE.

Saloojee, R., Groenewald, D., & Du Toit, A. S. A. (2017). Investigating the business value

 of information management. *SA Journal of Information Management, 9(1)*.

Saunders, M., Lewis, P., & Thornhill, A. (2017). Research methods for business student’s

 5th ed. *England: Pearson Education Limited*.

SC Jobs (2017). *Job Description: Chief information security officer*. Consulted in 18th

 March 2018. Available in [https://www.scmagazineuk.com/job-description-chief- information-security-officer/article/629762/](https://www.scmagazineuk.com/job-description-chief-%20%20%20%20%20%20%20%20%20%20information-security-officer/article/629762/)

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*, 333-339.

Soto-Acosta, P., Popa, S., & Martinez-Conesa, I. (2018). Information technology, knowledge management and environmental dynamism as drivers of innovation ambidexterity: a study in SMEs. *Journal of Knowledge Management*.

Taherdoost, H. (2016). Sampling methods in research methodology; how to choose a sampling technique for research. *How to Choose a Sampling Technique for Research (April 10, 2016)*.

Von Solms, B. (2001). Information security—a multidimensional discipline. *Computers &*

 *Security*, *20*(6), 504-508.

Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management

 perspective. *Computers & security*, *29*(4), 476-486.

Wolden, M., Valverde, R., & Talla, M. (2015). The effectiveness of COBIT 5 Information

 Security Framework for reducing Cyber Attacks on Supply Chain Management System. *IFAC-PapersOnLine, 48*(3), 1846-1852.

Zandani, S. (2016). *U.S. Patent No. 9,426,169*. Washington, DC: U.S. Patent and Trademark Office.

# Appendix 1: Survey Questionnaire

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Sr. No* | *Questions* | *Yes* | *No* | *Rarely* |
|  | **Please response to your responsibilities as CISO:** |  |  |  |
| 1 | Strategic security management  |  |  |  |
| 2 | Risk management in security plans |  |  |  |
| 3 | Providing training and awareness regarding security plans to the employees |  |  |  |
| 4 | Compliance of regulations and standards |  |  |  |
| 5 | Maintaining high data security |  |  |  |
| 6 | Procuring the technology by reviewing different security aspects |  |  |  |
| 7 | Develop the list of interested parties related to information security  |  |  |  |
| 8 | Teach employees how to perform risk assessment |  |  |  |
| 9 | Coordinate all efforts related to personal data protection |  |  |  |
| 10 | Propose the selection and deadline for safeguards implementation |  |  |  |
|  | **Enablers in performing responsibilities:** |  |  |  |
| 11 | Interpersonal support by employees |  |  |  |
| 12 | Cooperation and teamwork |  |  |  |
| 13 | Collaboration by all departments |  |  |  |
| 14 | Conflict resolution by regulations  |  |  |  |
| 15 | Advanced technologies  |  |  |  |
|  | **Hindrances in performing responsibilities:** |  |  |  |
| 16 | Hackers attacks by competitors via spy marketing to access the company’s data |  |  |  |
| 17 | Higher costs of advanced technologies |  |  |  |
| 18 | Centralized structure of organization which creates issues in taking timely decisions |  |  |  |
| 19 | Unfavorable behavior by employees |  |  |  |
| 20 | Lack of coordination among different departments of the organization  |  |  |  |

# Appendix 2: Interview Questions

* What are your core responsibilities as CISO?
* Do you assist in marketing intelligence of the business?
* What are the common factors, which help you in performing your responsibilities?
* How advancements in technology are affecting IT security plans? (Positively: by enhancing the strength and negatively: by equipping the hackers)
* Do you follow triage process in your IT security plans?
* What are the common threats you face in your IT security plan?
* What are the factors causing issues for you to perform your duties?
* How you would conclude the role of CISO in designing and managing the IT security plan of an organization?

# Appendix 3: Frequency Charts







































# Appendix 4: Frequency Table

| **RCISO1** |
| --- |
|  |  | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Yes | 14 | 70.0 | 70.0 | 70.0 |
| No | 3 | 15.0 | 15.0 | 85.0 |
| Rarely | 3 | 15.0 | 15.0 | 100.0 |
| Total | 20 | 100.0 | 100.0 |  |

| **RCISO2** |
| --- |
|  |  | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Yes | 17 | 85.0 | 85.0 | 85.0 |
| No | 1 | 5.0 | 5.0 | 90.0 |
| Rarely | 2 | 10.0 | 10.0 | 100.0 |
| Total | 20 | 100.0 | 100.0 |  |

| **RCISO3** |
| --- |
|  |  | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Yes | 18 | 90.0 | 90.0 | 90.0 |
| Rarely | 2 | 10.0 | 10.0 | 100.0 |
| Total | 20 | 100.0 | 100.0 |  |

| **RCISO4** |
| --- |
|  |  | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Yes | 11 | 55.0 | 55.0 | 55.0 |
| No | 3 | 15.0 | 15.0 | 70.0 |
| Rarely | 6 | 30.0 | 30.0 | 100.0 |
| Total | 20 | 100.0 | 100.0 |  |

| **RCISO5** |
| --- |
|  |  | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Yes | 10 | 50.0 | 50.0 | 50.0 |
| No | 4 | 20.0 | 20.0 | 70.0 |
| Rarely | 6 | 30.0 | 30.0 | 100.0 |
| Total | 20 | 100.0 | 100.0 |  |

| **RCISO6** |
| --- |
|  |  | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Yes | 17 | 85.0 | 85.0 | 85.0 |
| No | 1 | 5.0 | 5.0 | 90.0 |
| Rarely | 2 | 10.0 | 10.0 | 100.0 |
| Total | 20 | 100.0 | 100.0 |  |

| **RCISO7** |
| --- |
|  |  | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Yes | 14 | 70.0 | 70.0 | 70.0 |
| No | 1 | 5.0 | 5.0 | 75.0 |
| Rarely | 5 | 25.0 | 25.0 | 100.0 |
| Total | 20 | 100.0 | 100.0 |  |

| **RCISO8** |
| --- |
|  |  | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Yes | 15 | 75.0 | 75.0 | 75.0 |
| No | 2 | 10.0 | 10.0 | 85.0 |
| Rarely | 3 | 15.0 | 15.0 | 100.0 |
| Total | 20 | 100.0 | 100.0 |  |

| **RCISO9** |
| --- |
|  |  | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Yes | 9 | 45.0 | 45.0 | 45.0 |
| No | 11 | 55.0 | 55.0 | 100.0 |
| Total | 20 | 100.0 | 100.0 |  |

| **RCISO10** |
| --- |
|  |  | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Yes | 9 | 45.0 | 45.0 | 45.0 |
| No | 5 | 25.0 | 25.0 | 70.0 |
| Rarely | 6 | 30.0 | 30.0 | 100.0 |
| Total | 20 | 100.0 | 100.0 |  |

| **ENBLR1** |
| --- |
|  |  | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Yes | 17 | 85.0 | 85.0 | 85.0 |
| No | 2 | 10.0 | 10.0 | 95.0 |
| Rarely | 1 | 5.0 | 5.0 | 100.0 |
| Total | 20 | 100.0 | 100.0 |  |

| **ENBLR2** |
| --- |
|  |  | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Yes | 17 | 85.0 | 85.0 | 85.0 |
| Rarely | 3 | 15.0 | 15.0 | 100.0 |
| Total | 20 | 100.0 | 100.0 |  |

| **ENBLR3** |
| --- |
|  |  | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Yes | 19 | 95.0 | 95.0 | 95.0 |
| No | 1 | 5.0 | 5.0 | 100.0 |
| Total | 20 | 100.0 | 100.0 |  |

| **ENBLR4** |
| --- |
|  |  | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Yes | 15 | 75.0 | 75.0 | 75.0 |
| No | 3 | 15.0 | 15.0 | 90.0 |
| Rarely | 2 | 10.0 | 10.0 | 100.0 |
| Total | 20 | 100.0 | 100.0 |  |

| **ENBLR5** |
| --- |
|  |  | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Yes | 17 | 85.0 | 85.0 | 85.0 |
| No | 3 | 15.0 | 15.0 | 100.0 |
| Total | 20 | 100.0 | 100.0 |  |

| **HIND1** |
| --- |
|  |  | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Yes | 20 | 100.0 | 100.0 | 100.0 |

| **HIND2** |
| --- |
|  |  | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Yes | 18 | 90.0 | 90.0 | 90.0 |
| No | 1 | 5.0 | 5.0 | 95.0 |
| Rarely | 1 | 5.0 | 5.0 | 100.0 |
| Total | 20 | 100.0 | 100.0 |  |

| **HIND3** |
| --- |
|  |  | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Yes | 17 | 85.0 | 85.0 | 85.0 |
| No | 3 | 15.0 | 15.0 | 100.0 |
| Total | 20 | 100.0 | 100.0 |  |

| **HIND4** |
| --- |
|  |  | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Yes | 20 | 100.0 | 100.0 | 100.0 |

| **HIND5** |
| --- |
|  |  | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Yes | 17 | 85.0 | 85.0 | 85.0 |
| No | 2 | 10.0 | 10.0 | 95.0 |
| Rarely | 1 | 5.0 | 5.0 | 100.0 |
| Total | 20 | 100.0 | 100.0 |  |