Master Degree Project

UNIVERSITY OF SKÖVDE

The Challenges of Evaluating and Following Up on Information Security within Swedish Government Agencies:

A Qualitative Case Study

Birgitta Landelius

Supervisor: Ali Padyab
Examiner: Rose-Mharie Åhlfeldt

Master Degree Project (120 ECTS) in Informatics
30 ECTS
Spring term 2023

ACKNOWLEDGMENTS

I would like to thank my supervisor Ali Padyab for your support with this project. Your guidance has helped me to achieve my ambitions. I would also like to thank course examiner Rose-Mharie Åhlfeldt for your insights into the field, which were truly valuable.

I would also like to thank my additional supervisors Désirée Veschetti and Christoffer Schmid for your regular support this spring. Thank you both for pointing me in the right direction and connecting me with the right people.

Finally, thank you to all the informants who wanted to participate, much appreciated.

ABSTRACT

The digitalisation of society is rapidly progressing, but along with digitalisation, there are threats. Cyber attacks are a rising concern, especially for the public sector and government agencies. To resist attacks, it is crucial to establish a systematic information security work. Among activities within the systematic information security work, two of them are evaluation and follow-up. Those are activities important for the continuous improvement that should occur when working systematically. However, research has revealed that such activities are challenging to perform. Swedish government agencies have experienced difficulties for years with evaluating and following up on their information security work, although it is a requirement to fulfil. Therefore, this study aims at investigating how information security is evaluated and followed up within Swedish government agencies for civil preparedness by applying a qualitative case study.

The study used two methods to collect data. Data was gathered from public documents and a qualitative content analysis was performed. A total of 152 documents were analysed, including appropriation directions and annual reports. In combination, ten semi-structured interviews were conducted with informants from government agencies responsible for civil preparedness and individuals with extensive work experience regarding information security in the public and private sectors. The interview data were analysed similarly to the public documents, hence content analysis and categorisation into themes.

The results indicate that evaluation and follow-up of information security are performed, but they are burdensome for government agencies. It is mainly due to unclear requirements and weak governance. In addition, evaluation is a time-consuming and resource-intensive activity, which makes it challenging to motivate. The study enlightens these challenges, and its findings could be utilised in future research to aid the problem situation.

Keywords: Information Security, Public Sector, ISMS, Evaluation, Governance

Table of Contents

1. Introduction

Sweden has a reputation for being a country at the forefront of digitalisation. The country has been at the top of the European Commission's *Digital Economy and Society Index* (DESI) report for the past few years. In the most recent report, which was published in 2022, Sweden ranked in 4th place. The report measures various aspects of digitalisation efforts within each EU member state (European Commission 2023). However, in the 2020 Global Cybersecurity Index report by the *International Telecommunication Union* (ITU), an agency specialising in information and communication technologies, Sweden ranked 26th (ITU 2023). Concurrently, this fact can be seen as a contradiction because, in the Government Communication (2017/18:47), a goal was announced that Sweden should be the best country in the world in the use of the possibilities of digitalisation. The Government Communication (2017/18:47) explicitly mentions that the public sector should have considerable responsibility in providing services to support work towards the goal. Digital services intend to increase information sharing within the government offices, but also toward citizens (Thompson, Mullins and Chongsutakawewong 2020). The aforementioned picture of digitalisation in Sweden is shared in a recently published report by the *Agency for Digital Government* (DIGG). It also adds that digital services provided by the public administration are uneven (DIGG 2023). With non-functional information security work, organisations and agencies cannot provide services that are critical to society (Eugen and Petruţ 2019). Thus, as society becomes increasingly digitalised, the importance of performing information security work also becomes imperative and should not be neglected.

In 2017 a severe incident was discovered regarding the management of information security in the Swedish public sector. It became public that the Swedish Transport Administration had contracted IBM to provide services related to outsourcing the agency's IT system. At the time of the outsourcing decision, the Director General of the Transport Agency had disregarded certain parts of the Protective Security Act (SFS 2018:585) and other regulations. The agency's guidelines had been ignored as well. As a result, sensitive information was made available to unauthorised personnel living abroad. The information disclosure was considered detrimental to Sweden's national security (Transportstyrelsen 2023; SVT Nyheter 2019). The lack of information security capabilities within the Swedish public sector was also highlighted in a report by the *Royal Swedish Academy of Engineering Sciences* (IVA). Concerns were raised about whether political, governmental, and industry management are aware of the precarious situation. It was also suggested that all parts of Swedish society are potential targets, and that digitalisation equals exposure to cyber threats. Several observations in the report point to missing capabilities and insufficient preparation within several domains. Decision-making at the political level is inadequate in relation to the evolving reality of cyber threats, and requirements are not met. Furthermore, public-private cooperation is lacking, which will negatively impact emerging cybersecurity companies (IVA 2022). A recent report by the *Swedish Security Service* (SÄPO), on the current threat landscape in Sweden, makes a similar point.

There is a lack of security protection mechanisms in critical companies that manage information security, and security analyses are not carried out as required (SÄPO 2023a). Besides, with rapid changes in the technological environment, it is fundamental that organisations and agencies keep up to date with measures, as there is constantly an imminent risk of them becoming outdated (Williams 2001).

Having a functioning and implemented information security work is important. von Solms and von Solms (2004) discuss ten deadly sins of information security management. It is prevalent for all the listed sins that information security involves the entire organisation. Information security is not only a technical issue, but a business issue, and top management must understand it. In addition, the top management is responsible for ensuring that the information assets of the organisation are kept secure. Unsecured, compromised information assets can create bitter financial and legal dilemmas for the organisation. It is therefore vital to understand the multi-dimensional aspect of information security. In conclusion, the authors argue that it is important to learn what other organizations have achieved. Following best practice is wise, since there is no need to reinvent the wheel. The recently published report (RiR 2023:8) by the Swedish National Audit Office, which examined the Swedish government's governance of information security and cybersecurity, showed that the government has been working for several years in contrast to the success factors described above. The investigation aimed to see whether the government's work to strengthen information security and cybersecurity has been effective. The report concludes that the work is not considered effective. In addition, it was found that the Swedish National Strategy for Information Security and Cybersecurity lacks objectives that allow follow-up. As a result, government agencies have been forced to work according to their own objectives and priorities. Ultimately, this has made it difficult to evaluate the measures taken to strengthen information security and cybersecurity work (Riksrevisionen 2023). In particular, clear instructions from the governing actors are advocated by Horne (2018), who argues that an information security strategy should approach information security comprehensively but maintain clarity. In addition, implemented information security controls must be continuously monitored and audited for systematic work to improve (Steinbart, Raschke, Gal and Dilla 2012). As depicted, one of the main challenges, due to the immensity of information security, is to set relevant objectives and to evaluate and follow them up.

1.1 Problem Definition

As mentioned in the previous paragraph, Sweden is digitalised, but digitalisation also means exposure to cyber threats (IVA 2022). When carrying out their information security work, Swedish government agencies have regulations and guidelines to follow. For example, the *Swedish Civil Contingencies Agency* (MSB) has a provision (MSBFS 2020:6) on how information security work should be performed within government agencies. In addition, MSB provides a tool called the Method Support, which aims to help organisations and government agencies implement systematic information security work (Informationssäkerhet.se 2020). In recent years, however, several reports have found that Swedish government agencies do not comply with the regulations and guidelines. One of the reports,

compiled by MSB, was based on a survey called *Infosäkkollen*, which was conducted in the public sector. Municipalities, regions, and government agencies participated, and 122 government agencies responded to the survey. The results were categorised, making it possible to explicitly interpret the results for government agencies. The result showed that the majority of government agencies do not meet the desired requirements in MSBFS 2020:6. The guidelines in the Method Support are not being followed, and the work on information security as a whole is either lacking or non-existent. Information classification, which is a fundamental part of the Method Support, is not sufficient. In addition, only 50–75% of the security measures implemented are evaluated as to whether they are appropriate (MSB 2022a). The Swedish National Audit Office, in its audit report (RiR 2016:8), has also identified shortcomings in information security work within nine government agencies. Besides examining IT costs, governance and control were also measured and found to be lacking. It was particularly challenging to find any follow-up procedures concerning the *Information Security Management System* (ISMS). The lack of follow-up makes it difficult to carry out the continuous improvement work that should be undertaken when an ISMS is in place. Therefore, the report concluded that it is challenging to get an overview of the information security work in the audited government agencies and that the work is performed in different ways. However, it should be carried out similarly regardless of the government agency (Riksrevisionen 2016). Granted that 14 § in (MSBFS 2020:6) declares that the information security work within government agencies should be followed up and evaluated at least annually, but the reports show that there is a noticeable challenge for the government agencies.

Attacks are unpredictable in the current threat landscape (Yusif and Hafeez-Baig 2021), and various Swedish government agencies, among other critical businesses, are and have been subject to cyber attacks (SecurityUser.com 2023; Försvarsmakten 2022). So, with imminent cyber incidents, there must be resilience, meaning systems and organisations should be capable of combat such incidents (Boyes 2015). Therefore, systematic information security must function accordingly. In view of the previous information security incident involving the Swedish Transport Administration, it is clear that the information security work within Swedish government agencies needs to be improved. As mentioned above, and according to the Method Support (Informationssäkerhet.se 2020b), follow-up, evaluation, and improvement are one of the four core parts of systematic information security work. For this reason, the issues are worthy of attention and further investigation to find the cause behind the problem situation.

The contribution of this study is therefore to investigate how evaluation and follow-up procedures regarding information security are performed within Swedish government agencies. The findings intend to highlight potential challenges, or procedures working well. Among the 340 government agencies in Sweden (Regeringen 2023a), 39 of them are appointed with specific responsibilities for civil preparedness, and these agencies were selected as the focus of this study. The ordinance (SFS 2022:524) declares the readiness of government agencies, and in 18 § it is stated that the included agencies have a special responsibility due to their critical function for society. They are therefore obliged to carry out several activities, such as risk and vulnerability assessments. They should also report to the government and MSB on the development of relevant events (SFS

2022:524). Because of their importance to society, both in times of peace and in times of preparedness, they are considered to be relevant in the scope of this study. Furthermore, government agencies had some of the lowest scores in *Infosäkkollen* (MSB 2022a). Existing regulations and guidelines, including appropriation directions, ordinances, and guidelines, appear insufficient for government agencies to carry out systematic information security work. Particularly evaluation and follow-up seem to be among the greatest issues. In addition, there has been limited research focusing on aspects of evaluation and follow-up, thus making it a compelling area to investigate.

1.1.1 Research Question

The proposed research question the study aims to answer is defined:

- How is information security evaluated and followed up in Swedish government agencies for civil preparedness?

1.2 Delimitation

There are 60 agencies with specific responsibility for civil preparedness. These include the 21 county administrative boards (MSB 2023a). However, the study has chosen to exclude the county administrative boards and solely focus on the 39 government agencies. The choice is motivated by the crucial role that government agencies play, and by the fact that the Swedish principle of public access allows access to official documents relevant to the study. In addition, it may be easier to compare the results if only one type of organisation is studied, namely government agencies. It is worth noting that the agencies have not been officially designated as responsible for civil preparedness until 1 October 2022 (MSB 2022e). However, this fact does not affect the study and the documents examined, as the scope of the agencies is only a delimitation.

The similarities between information security and cybersecurity are and have been widely debated. The two terms are often used interchangeably. While information security is about protecting an asset, that is information, cybersecurity is also about protecting cyberspace as a whole. Cyberspace includes several aspects, such as the people operating in cyberspace and their assets. Consequently, cybersecurity is about protecting these people and their assets (Reid and van Niekerk 2014). Cybersecurity also includes the infrastructure and networks that need to be protected (MSB 2021a). Therefore, for the scope of this study, the term information security is the main focus, as it is the systematic information security work within government agencies that is investigated.

1.3 Thesis Structure

The remaining parts of the report, the work is structured as follows: in Chapter 2, the background will be provided including relevant preliminaries and previous research, Chapter 3 will describe the chosen method, Chapter 4 will present the results, and Chapter 5 focus on the discussion around the findings, lastly, in Chapter 6 the conclusion will be summarised.

2. Background

This section presents preliminaries relevant to the study, it also presents research that has previously been carried out within the field.

2.1 Preliminaries

The following section presents several concepts that apply to the study. Information security is first explained in general terms and then narrowed down to describe it in the context of the Swedish public sector. In addition, the governance of government agencies is outlined to provide an understanding of how information security is governed and controlled. The section concludes with definitions of some regulations related to information security. Regulations, agencies, and other terms related to the public sector have been translated utilising the multilingual dictionary of the Swedish Parliament (Riksdagsförvaltningen 2020).

2.1.1 Information Security

Information security used to be a technical term, but over the years, the term has expanded, and definitions have been provided from other research fields (Horne, Ahmad and Maynard 2016). Thus, different opinions on how to define information security have been a subject of discussion in research. Siponen and Oinas-Kukkonen (2007) argue that researchers from contrasting disciplines have not put enough effort into studying information security, apart from their discipline. As a result, it has been challenging to obtain a comprehensive view of information security. According to the *International Standardisation Organisation* (ISO), the official definition of information security is "the preservation of the confidentiality, integrity, and availability of information" (ISO/IEC 27000:2018, 3.28). The three concepts in the definition form the CIA triad, where confidentiality means protecting information from unauthorised access. Integrity means that information should not be altered and should retain its validity. Finally, availability means that information should be accessible to authorised individuals when it is needed (Warkentin and Orgeron 2020). By maintaining confidentiality, integrity, and availability, information security aims to maintain business continuity and mitigate potential security incidents. It is possible to view information security as a process in which organisations and the people involved seek to capitalise on and enhance the value of information. To extract value from information, it is necessary to apply appropriate controls to protect the information from various threats. By doing so, the intended purposes of the information can be achieved (Horne, Ahmad and Maynard, 2016). Consequently, information is considered an asset that needs to be protected from any misuse and harm (von Solms and van Niekerk 2013).

The definition and objective of information security are equivalent to the public sector, where it is identically or even more critical to protect information. The Swedish National Strategy for Information Security and Cybersecurity can be found in Government Communication (Skr. 2016/17:213). In the communication, information security, and cybersecurity are used interchangeably, but for the purpose of this study, only the term information security is used to describe the content of the communication. The general objectives for the national security of Sweden are the basis on which the strategy for information security is laid

down. The objectives are to protect the lives and health of the population, maintain the functioning of society and defend democratic rights and values. To defend these values, information and the systems that handle it must be protected. To reap the benefits of digitalisation, information security must be considered a fundamental function. Information should be accurate and easily accessible to all individuals. However, some information is considered sensitive and must be protected. Information relating to the functioning of society and sensitive information relating to privacy is particularly important to protect. Supposing it were to be disclosed to unauthorised entities or manipulated, the consequences could be serious. Both public and private functions and systems depend on information and communication technologies and therefore need protection. The Government Communication also states that protection is the responsibility of society as a whole, both government agencies and private organisations. In order to maintain an acceptable level of information security, the work must be carried out in a systematic way. Systematic information security work means that the work is performed collectively and uniformly (Skr. 2016/17:213).

2.1.2 Systematic Information Security Work

In the context of this study, it is relevant to briefly define systematic information security work. The term is generally understood to mean working in a predetermined way that ensures the organisation has all the necessary steps employed to identify important information and how to protect it. Combined with a risk-based way of working, information will be better used, and the cost of protecting information will also be kept at a reasonable level (MSB 2022b). The tool Method Support, mentioned above and provided by MSB, consists of four steps to follow to achieve a systematic way of working with information security. The steps are based on best practice, and the tool itself is based on the international standard family ISO/IEC 27000 (Informationssäkerhet.se 2020a). In addition, standards are given considerable consideration in systematic information security work, and organisations of all kinds benefit from following appropriate standards as they are based on proven ways of working (SOU 2015:23). As there are obvious challenges in creating a sound way of working with information security, the support aims to equip organisations with the necessary tools to achieve the desired work. It means that the support explains in great detail how to carry out certain activities. The first step is to identify and analyse, the second is to design, the third is to implement and the fourth is to monitor and improve. By performing each of these steps, the organisation will have a systematic approach to information security. To exemplify, the identify and analyse step involves carrying out various analyses such as environmental analysis and risk analysis. During the design phase, governing documents are created, for instance, the information security policy. This policy should be the overarching document depicting the management of information security in the organisation. In the use step, the organisation should start to comply with the documents produced in the previous step. Finally, follow-up and improvement involve controlling and measuring the results to observe the extent to which the information security objectives are met (Informationssäkerhet.se 2020a). Working systematically with information security is a process and should be carried out continuously to ensure compliance with the governing documents (MSB 2015).

Working systematically with information security often becomes easier if the organisation implements an ISMS. It is not a technical system, but a management

system. Therefore, it is the top management that should initiate the implementation of the system. Top management must believe in the benefits of implementing an ISMS. It has been assumed that technical mechanisms provide the greatest protection for securing information. However, it is equally important that the people and processes involved carry out their work according to established procedures. To create a secure environment within an organisation, all elements and situations need attention. The ISMS provides a comprehensive view of how to create an organisation that can protect its information. Aspects to be considered are legal, human, technical, policy design, and more. The ISMS also aims to establish a security culture within the organisation, and often this process can be challenging. It is therefore fundamental to carry out audits of the ISMS to verify the compliance of the controls implemented. ISO/IEC 27001 is the standard to follow when implementing an ISMS, and if all the requirements in the standard are met, an organisation can be certified against it (Broderick 2006; Eloff and Eloff 2003). Concerning Swedish government agencies, the provision (MSBFS 2020:6) requires government agencies to implement an ISMS and to consider ISO/IEC 27001:2017 and ISO/IEC 27002:2017 in this work (Informationssäkerhet.se 2020c).

2.1.3 Governance in the Swedish Public Sector

The Instrument of Government (SFS 1974:152) is one of Sweden's four fundamental laws and defines the form of government. It states that Swedish public power emanates from the people. The Instrument of Government also defines the governance of the country, the democratic rights of the people, and the distribution of public power (Sveriges Riksdag 2022). There are about 340 government agencies that serve under the Swedish government. They are responsible for implementing the decisions taken by the government and parliament. Except for the government itself and the Swedish courts, government agencies are also named administrative authorities because they serve the government. In addition, the agencies are of different sizes and operate in a wide range of areas. The agencies carry out the practical work required based on political decisions taken by the government (Regeringen 2023a).

Government agencies are considered independent, but they are not autonomous as they are controlled by the government. Each agency forms its organisation with managers and employees, although it is usually the government that selects the top administration. The agencies can make independent decisions without the involvement of the government; these decisions usually concern the exercise of authority over a municipality or the application of law (Regeringen 2023a; SFS 1974:152). The ordinance on administrative authorities (SFS 2007:515) also explains how the administrative authorities should organise their work in terms of administration, tasks, decisions, and cooperation with the EU, and applies to all administrative authorities.

Of all the ways in which the government can control the administrative authorities, the most fundamental is the appropriation direction. These are issued to each administrative authority in December of each year and come into force on 1 January. An extensive part of the appropriation direction describes the funding the agency has received for the year and how the money should be allocated. But the letters also describe how the agencies should carry out their work in the coming year, and sometimes there are specific tasks and objectives that the agency

should achieve. At the end of the year, the agency summarises its work and submits an annual report for the government to follow up on and evaluate. To further evaluate the results of each agency, government representatives and the agency's administration have an annual meeting where they discuss the agency's ongoing work and improvement (Fortifikationsverket n.d.; Post- och telestyrelsen 2022; Regeringen 2023a). Another decision used by the government to control the administrative agencies is an instruction specific to each agency. The instructions define specific tasks that the agency should perform, but the instructions are not assigned annually, hence they are fixed and do not change compared to the appropriation instructions (Regeringen 2023a).

2.1.4 Information Security and Government Agencies

Having briefly described the governance of Swedish government agencies, it is time to enter the context of the study by defining how information security is governed in the public sector. Although there are several government agencies in different areas, Sweden does not currently have a dedicated agency that manages information security and cybersecurity issues. A fundamental point in the National Strategy for Information Security and Cybersecurity articulates the importance of ensuring a unified approach when working with information security (Regeringen 2023b). As there is no dedicated government agency managing information security issues, the responsibility has been assigned to several agencies. In addition, several agencies have created constellations for cooperation in the information security domain. For example, seven agencies are members of the *Cooperation Group for Information Security* (SAMFI), in which all agencies have specific responsibility for information security in society. The work consists of a collaboration between the agencies, where they support each other and exchange information and experience. The agencies involved are the MSB, the *Swedish Post and Telecom Authority* (PTS), the police, the *Swedish Defence Radio Establishment* (FRA), SÄPO, the *Swedish Defence Materiel Administration* (FMV), and the Swedish Armed Forces (Informationssäkerhet.se 2015).

An initiative in cooperation between government agencies to improve information security is the *National Centre for Cybersecurity* (NCSC). It was initiated on behalf of the government in December 2020 and the FRA, the Swedish Armed Forces, MSB, and SÄPO are the initiators, but work closely with the police, FMV, and PTS. The aim is to improve and create a thorough resistance with a special focus on the prevention, detection, and management of cyber threats. By working together, the agencies' capabilities will be strengthened, and they will receive support with their tasks. It will make it easier for agencies to share information and coordinate their work in the event of a cyber incident. The centre also hopes to improve the overall cyber capability of the private sector, hence focusing on inter-organisational cooperation (MSB 2021b; MSB 2022c). When announcing the centre, it was to be operational in 2025. However, following criticism of the uncertainties in the development process, the Swedish government announced in April 2023 that the centre is given a new start, with only the FRA responsible for the work (DN 2023).

2.1.5 Regulating Information Security

Information security in Sweden is governed by a number of regulations. The regulations are different and there are differences in their mandatory force. Laws,

ordinances, and rules have a legal basis and must be followed. The creation of a law begins with a proposal from the government, and the parliament then decides whether to enact the law (Folkhälsomyndigheten 2022). With regard to information security, the Information Security for Socially Important and Digital Services Act (SFS 2018:1174) is based on the *Directive on Security of Network and Information Systems* (NIS), which is constituted by the EU. All EU members must follow the directive, so the NIS directive has been implemented into Swedish law. Seven sectors are covered by the directive since they are considered to have a critical importance to society. The sectors are banking, digital infrastructure, energy, financial market infrastructure, health care, drinking water supply, and transport. As a result, Swedish government agencies in these sectors are obliged to comply with (SFS 2018:1174). The purpose of the act is to achieve a high level of security within information systems and networks. In January 2023 the new directive NIS2 was enforced, improving cybersecurity measures within EU member states. Several sectors were added, now also including the public sector. By November 2024 all members must have NIS2 incorporated into their respective legal framework. Currently, Swedish government agencies are evaluating whether they will be covered by the new directive (Enisa n.d.; Informationssäkerhet.se 2020c; MSB 2022d). There is also the Protective Security Act (2018:585), which regulates how to protect confidential information that is sensitive to Sweden's national security. The act aims at organisations that manage confidential information.

There are also ordinances. The government decides on ordinances, and they can be defined as a compliment or clarification to laws. For instance, the law mentioned above (SFS 2018:1174), has the ordinance (SFS 2018:1175). It is described as a complement to the law on Information Security for Socially Important and Digital Services. It also explains preventive measures and how to carry out certain actions related to the protection of information security. Similarly, the Protective Security Act (2018:585) has an ordinance (SFS 2018:658), in which the third chapter is dedicated to information security and the protection of information systems and their requirements.

Finally, there are rules to follow. In contrast to ordinances, rules are even more detailed and often explicitly describe how to fulfil requirements set out in the laws. They generally cover a specific area of regulation. Rules are decided and prescribed by government agencies, but there must be an authorisation in the regulation for the government agency to decide on a rule (Folkhälsomyndigheten 2022; Informationssäkerhet.se 2021). MSB issues (MSBFS 2020:6), which describes the systematic information security work based on ISO/IEC 27001 and ISO/IEC 27002 that government agencies must follow. The 14 § states that information security work within an agency must be followed up annually. Methods for performing the work, internal rules, information classifications, and risk analyses, to name a few, are activities to be evaluated. In addition, (MSBFS 2020:7) is similar to (MSBFS 2020:6), although it specifies how government agencies manage information security within information systems. The focus is therefore slightly more technical than (MSBFS 2020:6).

The regulatory measures for information security mentioned above apply to the context of this study. Considering the above, MSB is the government agency with the most comprehensive responsibility for information security (Turell, Su and

Boulanin 2020). The public sector recognises information security, but it is worth noting that evaluation and follow-up are only briefly mentioned in the regulatory mechanisms. In addition, MSB only has the authority to issue regulations, but it has no jurisdiction to impose fees if regulations are not complied with.

2.2 Research Background

Information security in the public sector is a widely researched area. However, to the author's knowledge, there has been little research into systematic information security work and how it is followed up and evaluated in public organisations. By looking at what has previously been achieved in this field, the report will cover various research areas related to systematic information security work. In addition, terms and activities mentioned in the Method Support, which have a direct connection to systematic information security work have been considered in the examination of previous research. The focus will have both a global and a Swedish perspective in an attempt to give a broad picture.

The size of the public sector varies from country to country. However, the general structure is often similar. In almost all countries the public sector is responsible for managing functions that are critical to society. There is a wide range of essential functions where the public sector must deal with everything from the economy to energy and health services (Loukis and Spinellis 2001). In addition, a large amount of sensitive data is managed, so citizens' information and privacy must be protected. Therefore, different government agencies and departments within the public sector must work together to administer this information in the most applicable way (Bigdeli, Kamal and de Cesare 2013).

2.2.1 Information Security Policy

The information security policy could be considered a limited part of systematic information security work. However, the design and implementation of this policy are part of the Method Support. It is therefore compatible to examine previous research on information security policy to find possible clues as to why systematic information security work is insufficient in terms of evaluation and follow-up within the Swedish public sector.

In literature, the information security policy has been defined in various ways. It has been described as a high-level document, but also a meta-document describing how the policy should be implemented. However, Bergström, Anteryd and Åhlfeldt (2020) argue that for information to be considered equally, it is important to acknowledge that the information security policy is a high-level document that concerns the entire organisation. Different interpretations of what constitutes an information security policy seem to be a source of implementation challenges. Paananen, Lapke and Siponen (2020) suggest that it would be beneficial to establish a unified meaning of the term. One of the main sources of confusion is that the information security policy is defined as different documents depending on the organisation involved. For example, a distinction should be made between what the information security policy describes and what its functions are. So what the policy is must correspond to what it does. There should also be a plan for how revisions to the policy will be carried out. Changes to the policy should not be made only because an incident has occurred, by which time

it is too late as information has most likely been disclosed or harmed. Stafford, Deitz and Li (2018) share the view on the information security policy, but they extend it by arguing that the policy should state how the company's information will be secured and how objectives will be met. The document can also be considered the basic level on which audits are conducted. Based on the audit findings, information security improvements can be proposed.

Karlsson, Hedström and Goldkuhl (2017) conducted a study in a Swedish county council reviewing three information security policy documents. An information security policy is crucial for an organisation. For instance, it specifies how employees should perform their work with the applicable security measures. The study resulted in eight criteria, all aimed at improving the design of an information security policy. The authors conclude by stressing the importance of creating a policy that is useful to employees and that management recognises the needs of employees. Similarly, Stahl, Doherty and Shaw (2012) conducted a study in the UK national healthcare sector, investigating the role and purpose of information security policies. The findings suggested that for an information security policy to be successful, it should be created locally with the participation of employees. Writing policies using terminology that is easy to understand, but also addressing issues raised by employees will consequently facilitate policy adoption according to the authors. Involving employees were also found to be positive in mitigating the challenges of turning policy into practice. Hedström, Kolkowska, Karlsson and Allen (2011) investigated the phenomena in a Swedish county hospital and concluded that employees should be involved in the process of creating information security controls. In addition, management should recognise information security in relation to the whole organisation, and therefore it should be a strategic issue. A survey of several municipalities in the United States found that while several municipalities have an information security policy in place, there are several areas where improvements could be made. For example, policies should be reviewed on a regular basis, preferably by an external auditor; the study found that this activity was uncommon, hence the need for improvement. In addition, policies were not integrated into day-to-day operations (Hatcher, Meares and Heslen 2020). Similarly, US local governments were surveyed to outline the need to ensure high levels of cybersecurity. The main findings suggested increased funding for cybersecurity, better policies, and increased cybersecurity awareness among employees (Norris, Mateczun and Joshi 2019).

2.2.2 Effects of Information Security Standards

As the Method Support tool, based on ISO 27001 states that an ISMS should be implemented in accordance with ISO 27001, the following studies are of interest to show the effects of following the standard or being certified to it. Most research has focused on private organisations, but as the standard should be similarly implemented by organisations, the research could indicate that the results apply to public organisations. It can be concluded that there is a lack of research on evaluation, follow-up, and improvement of the work that should be done according to ISO 27001.

The ISO/IEC 27001 standard is designed to have a broad scope to make it easier for organisations to implement. The argument is that because of its broad scope,

organisations of all types and sizes can implement it (ISO 2018). However, Siponen and Willison (2009) argue the opposite. They examined a number of information security management standards, and their findings show that these standards were formulated universally. Therefore, the standards did not account for organisational differences and security requirements. Thus, universal measures could be applied to security issues, and it was argued that in some cases security measures were not applied at all because of their generic nature. Boehmer (2008) took the argument to the point of claiming that an implemented ISO/IEC 27001 ISMS do not necessarily say anything about the performance and quality that the implementation has produced. In addition, a review of the literature on ISO/IEC 27001 showed that there has been limited interest in studying the standard. Among the key findings, it was suggested that there is a lack of evidence of the consequences of certification to the standard. The authors also argue that academia has perceived ISO/IEC 27001 as a topic regarding technical aspects, but the standard is also about the management side of information security. The authors, therefore, call for a change of perspective (Culot, Nassimbeni, Podrecca and Sartor 2021). Ganji, Kalloniatis and Mouratidis and Malekshahi Gheytassi (2019) also ask for further research on the implementation of ISO/IEC 27001. In their study, they found little previous research that provided suggestions on how to meet all the requirements of the 27001 standard and therefore argued that the studies were incomplete in this regard. Of the 22 requirements in the standard, some have received less attention than others. The authors found that "Internal audit", "Management review", and "Continuous improvement" were among those categorised as having little or no prior research. At the same time, when Park, Jang and Park (2010) looked at the impact on an organisation's ISO/IEC 27001 certification, the results often focused on the business impact in terms of economic aspects. These include positive improvements in customer and public relations. Another study, albeit with a focus on ISO 9001, which addresses quality management, looked at how to increase the value of internal audits. The study, which was based on a literature review, found that previous research had focused on compliance, but lacked improvement aspects. Directions for future research were suggested, including a desire to highlight opportunities for improvement and what an organisation needs to achieve this work (Lenning and Gremyr 2021).

2.2.3 Aligning Information Security with Organisational Objectives

In addition to having a policy, other procedures must be in place to be capable of governing information security within an organisation. A literature review by AlGhamdi, Win and Vlahu-Gjorgievska (2020) derived several critical success factors for an organisation to govern its information security. Hedström, Kolkowska, Karlsson and Allen (2011) highlighted the importance of top management perceiving information security as a strategic issue. The findings of AlGhamdi, Win and Vlahu-Gjorgievska (2020) support the view by arguing that there should be an alignment between the organisation's objectives and the regulatory information security documents. Among the critical success factors, one is named "Assessment (Auditing)", the category consists of activities that the organisation should perform. For example, policies and procedures should be evaluated, the alignment between business and security controls should be assessed, and third-party audits should be performed. However, no further explanation was given as to how these activities should be carried out. Similarly, Posthumus

and von Solms (2004) argue that top management must prioritise information security and that this responsibility must involve the organisation's board of directors. Managing information security is complicated and all individuals in an organisation must be committed to protecting information assets. Top management is responsible for ensuring that the organisation complies with appropriate regulations and guidelines. It should also include information security policies, as failure to comply could have legal or financial consequences. Therefore, making information security a corporate interest will improve the overall operations of the organisation. Tu and Yuan (2014) identified critical success factors in information security management in their study. Aligning the business with information security management was found to have a positive impact on the overall information security work. For example, employees' IT knowledge increased, and with improved organisational support, security controls, and overall information security management performance also increased. Accordingly, MSB (2023b) also recommends prioritising systematic information security work.

2.2.4 Management of Information Security

Quite some years have passed since the publication by Eloff and von Solms (2000), who were early in highlighting the importance of managing information security holistically, focusing not only on technical aspects but also on how to manage processes and procedures. In another study, public administration institutions in Poland were the research subject regarding information security management. The results suggest that there are several issues related to information security management. For instance, the ISMS documentation was outdated, there was a lack of risk analysis. Further, reviews, audits, and controls were missing. Improvements and development of ISMS work were suggested, with the main recommendations, also relevant to this study, being improved ISMS audit methodologies and increased cooperation and sharing of experience between institutions. In general, the authors suggested the ISMS work be improved by increasing the systematic approach to it. To conclude, the authors wished to see future research in this area, as public authorities in particular play a major role in the development of digitalisation (Szczepaniuk, Szczepaniuk, Rokicki and Klepacki 2020). The concept of continuous improvement of information security management can generally be described as ongoing measures to protect information assets, increase the effectiveness of information security and monitor risks to minimise or mitigate them. The authors claim that organisations lack the motivation to continuously improve their security management and that it is unknown why. Also, the literature within the area has provided limited insight (Ghahramani, Yasdanmehr, Chen and Wang 2022). The best way to define the scope of an ISMS was discussed by Broderick (2006). The scope should not be broad, rather organisations should consider what the minimum requirements are to comply with a regulation. Having assessed the ISMS approach, they should also consider whether they can achieve compliance with their information security policy. Until they can answer this question in the affirmative, they will need to broaden the scope of the ISMS.

2.2.5 Information Sharing and Inter-Organisational Collaboration

An organisation can gain value by sharing information. By having the right information at the right time, information can be derived into knowledge. Information sharing requires technology to exchange information between different platforms that also have different governance structures. Sharing information

can bring benefits to both organisations involved, such as operational efficiency. For a public organisation, the aim is to provide services to the public, and by engaging in information sharing, the collaboration between agencies is facilitated and they can learn from each other (De Tuya and De Tuya 2019).

A study conducted in the Netherlands with public sector organisations working together revealed the need to implement security controls to carry out these procedures. In particular, challenges arose in establishing security controls that covered several public sector organisations. Further training of employees was also considered necessary to maintain relevant security controls (van Veenstra and Ramilli 2011). Further challenges were identified by Karlsson et al. (2021), who investigated the challenges of inter-organisational information sharing in the public sector. They argue that conflicting values within organisations can affect information-sharing practices. One of the key findings was that if an organisation's information is not shared or utilised following the organisation's values, there is a high risk that the organisation will attempt to change the whole of inter-organisational information sharing, making information-sharing practices dysfunctional. Inter-organisational cooperation has also been studied in Swedish government agencies with a focus on crisis management. Many of the agencies are now among those responsible for civil preparedness. From an organisational perspective, several success factors have been identified. These include the areas of clear governing documents and tasks, knowledge of the benefits of cooperation with other organisations, and decision-makers having the right knowledge of how to manage inter-organisational cooperation (Ödlund 2007). The positive aspects of inter-organisational cooperation are shared by MSB (2023b), which argues that cooperating increases efficiency and quality. However, difficulties could arise if government agencies share information on a cooperation platform that is accessible to external actors. Shared information could become public documents, which could reduce the willingness to cooperate as agencies fear exposure when sharing information.

Although some of the above reports do not explicitly consider information security, the inter-organisational approach is relevant as cooperation between government agencies has shown positive effects. Potentially, the benefits could apply to information security as well.

2.2.6 Different Information Security Perspectives in the Public Sector

Differences between the public and private sectors are evident when considering digital transformation. Jonathan (2020) identified critical success factors for digital transformation in the public sector and found that a combination of complex decision-making and stakeholder relationships are among the key challenges for the public sector. As IT investments are based on political decisions, informed management decisions are sometimes lacking. Plesner, Justesen and Glerup (2018) argue that digitalisation in the public sector must be recognised as a constant reform. The focus cannot solely be on technological aspects but organisational strategies and working methods, such as agile working, must be considered and implemented. Once again, knowledge sharing is advocated, and the authors argue that the potential of knowledge sharing has previously been overlooked. The success of the Danish e-government strategy was highlighted in the report by Meyerhoff Nielsen (2019), who found, for example, that strategy,

goals, and outcomes were well aligned across all government departments. In addition, they were good at performing a continuous assessment of different projects, thus conducting cycles of improvement. Combining this approach with clear key performance indicators was deemed to be a good approach. The public and private sectors were investigated in terms of information security awareness. Notable findings suggest that establishing a security culture is equally important in both sectors. Top management support also plays an equal role in both sectors. It is also suggested that information security activities within the public and private sectors have a positive impact on employee information security awareness (Khando, Gao, Islam and Salman 2021).

Research has also been carried out in the public sector in different countries. Although information security has been the main theme, different approaches have been explored. Some research is presented below to illustrate what is currently known. Information security in Ecuadorian public organisations was studied by (Izurieta, Jhony Caucha Morales, Toapanta Toapanta, Gallegos and Orizaga Trejo 2021) and found that the overall level of information security was low. The data and information security governance of three South African national government departments was analysed. The results showed a strong focus on protecting IT systems, but a lack of overarching information security governance skills, policies, and practices within government departments (Masilela and Nel 2021). A study conducted in Ethiopia, within one of the most digitalised ministries, showed a lack of information security work, with staff having little knowledge of information security policy and no training for staff (Jonathan, Hailemariam, Gebremeskel and Yalew 2021).

The level of information security in Swedish municipalities was investigated. The result showed that municipalities need support and tools for their ISMSs to increase systematic information security work. In general, the requirements imposed by the government are not fulfilled. The study could not conclude a single reason, but several, and the focus should be on what improvements can be made. The authors made several suggestions for improvement, where an information security policy and other governing documents should be established. In addition, there should be clear lines of responsibility in organising information security. Training should also be provided for all employees within the municipality (Åhlfeldt, Nohlberg, Söderström, Lennerholth and van Laere 2018). A model for information classification was derived for Swedish municipalities. The model was considered suitable for municipalities and other similar organisations. As with the previously described research, the authors emphasise the importance of examining existing policies and other guidelines so that information classification can be carried out accordingly (Bergquist, Tinet and Gao 2021). Also worth noting is that the information security policy is mentioned as a single document, so an organisation should not have multiple policies regarding information security. A study was conducted on Swedish government agencies and their information classification policies. The results showed that information classification is poorly performed, even though it is mandatory, and that government agencies struggle to implement the required policy (Bergström, Anteryd and Åhlfeldt 2020).

FOI investigated the lack of IT incident reporting in Swedish government agencies and the result suggested several reasons for the low reporting rates. Based

on the result, four areas were derived in which internal routines, internal conditions, perceived benefits, and implementation played a role. Each area then had several problems associated with it. To name a few problems, these included a lack of routines for transferring sensitive information, agencies not experiencing benefits from reporting incidents, and insufficient feedback from MSB. In addition, agencies had difficulty assessing the severity of IT incidents, and internal routines for identifying, documenting, and reporting incidents were missing or inadequate. Participating agencies were also encouraged to provide open-ended responses on potential improvements that MSB could make to improve IT incident reporting. One of the main improvements suggested was feedback from MSB. The monthly feedback report provided by MSB and sent to the agencies should be more detailed about the events and threats that MSB has received. By expanding the content of the feedback report to include reasons for incidents and vulnerabilities, agencies hoped to learn from each other. Agencies also want direct feedback from MSB on their reporting, including suggestions for improvement and how to follow up on these improvements. As there is no direct feedback from the MSB, the agencies experience that their reporting has only statistical significance (Stenérus Dover, Bengtsson and Olsson 2020).

What unites these findings is the lack of follow-up and evaluation of information security. Previous research has highlighted important aspects of information security such as policy, management, and information sharing. However, while these are important parts of systematic information security work, they do not address the requirements needed to improve evaluation and follow-up.

3. Method

This section presents the method choices for the study. It starts with the research approach, followed by the motivation of the sample selection. Then, data collection and data analysis procedures are accounted for. Thereafter, relevant research reliability and validity aspects are discussed. Lastly, ethical considerations are elaborated.

3.1 Research Approach

Based on the aim of this study, which is to investigate how information security is evaluated and followed up in Swedish government agencies, a number of objectives are derived. Berndtsson, Hansson, Olsson and Lundell (2008) generally describe objectives as sub-goals to achieve the aim. Accordingly, the overall objectives to perform are to first obtain public documents related to the 39 government agencies. The public documents are the distributed appropriation directions to government agencies for the years 2021 and 2022. They state how government agencies should carry out their work, and the directions can also include specific tasks that the agency should carry out. Also, the annual reports for the same years will be examined. Thereafter an analysis of the documents to get an understanding of how information security is evaluated and followed up will be carried out. Ten informants who can contribute with qualitative information will be asked to participate in the study. The obtained results will then be analysed to achieve a comprehensive view of the aspects of evaluation and follow-up regarding information security within Swedish government agencies for civil preparedness.

As the research background indicates, the field of information security is broad. Although technical aspects are not the focus of this study, the field encompasses governance, management, and individuals involved in information security work. This study also examines aspects of regulation and political governance, which is why the inductive research approach is chosen, combined with qualitative methods. In contrast to the inductive approach, the deductive approach focuses on testing the existing theory by deriving a hypothesis which is later tested against the empirical research (Saunders, Lewis and Thornhill 2007). Since there is limited knowledge about information security evaluation and follow-up in the public sector, especially in Sweden, and little previous theory is found, the inductive approach is considered appropriate. In the inductive approach, the aim is to understand specific circumstances, thus reality serves as the origin of the research. Through various observations, data is collected and later analysed, and the final step is to create or develop new theories (Saunders, Lewis and Thornhill 2007). As no previous theory is being tested in this study, observations of reality in the form of content analysis of documents and interviews are the starting points for the research. One can argue that the study has some deductive parts, as the concepts gathered in the research background are likely to serve as a ground for deriving themes during coding.

When using the inductive research approach, combining it with a qualitative case study is a common strategy (Patel and Davidson 2019). The case study is applicable when a complex problem needs recognition by gaining a thorough understanding and highlighting the problem from multiple perspectives (Crowe et al. 2011). Because the study will examine the stakeholders involved, which are the

government agencies, but also the governing documents, the qualitative case study is deemed appropriate. In addition, the case study is well suited when the research question aims to gather information that can be categorised as explanatory to answer the question. Often the questions are how, what, and why (Crowe et al. 2011). Recalling the research question for this study, "How is information security evaluated and followed up in Swedish government agencies?", the case study strategy hopes to provide in-depth data that can answer the research question. Another focus of the case studies is the extensive collection of data, which can come from individuals or programmes and usually includes interviews, observations, or documents. Sometimes the researcher also interacts with individuals at the site in question, the time spent there may be continuous over some time (Leedy and Ormrod 2015). However, this is not possible in this study due to the difficulty of spending time in different government agencies.

It is not uncommon for case studies to be the subject of criticism, the main concern being that their findings may be difficult to generalise. Yin (2013) argues that generalisation of case studies should be performed analytically or conceptually. The generalisation should account for whether the evaluated initiative produces a result, and the account should be seen as a form of theory. The result should not only be different concepts, but the produced theory should provide a better understanding of the investigation undertaken. The produced result or theory should then be linked to the existing literature, thus serving as an explanation for the gaps and potential shortcomings in this literature. This approach can mitigate potential limitations or challenges in generalising from a single case study, interpret the research with greater significance, and derive new knowledge. The study of information security evaluation and follow-up in Swedish government agencies may raise issues of generalisation. Potentially, the result could be specific to the sampled government agencies and therefore difficult to generalise to other agencies. However, this study follows a similar approach as described above by (Yin 2013). After conducting an extensive research background investigation with various information security concepts related to this study, the aim is to connect the result with existing research to create a new and thorough understanding of the research problem.

Another reason for the challenge of generalisation is that a case study often only examines a single case (Bell 2016). However, Yin (2013) recognises that they are useful in providing an in-depth explanation of a particular phenomenon. It can be considered contradictory, therefore Saunders, Lewis and Thornhill (2017) argue that it is the responsibility of the researcher to show that the findings of the study can be related to existing theory, thus explaining its significance. As mentioned above, the extensive research background will make it possible to associate the findings with previous research, but also fill the gap that is currently existing within the field.

3.2 Sample Selection

This section provides insight into the selection of public documents and informants, and how the choices are motivated.

3.2.1 Selecting Public Documents

The selected documents that will be part of the document analysis are public documents provided by the government and sent to all Swedish administrative agencies. The documents are appropriation directions sent to the agencies with special responsibility for civil preparedness. The documents are chosen because it is the most powerful tool for the government to control the administrative agencies operationally (Post- och telestyrelsen 2022). The agencies should therefore carry out their work accordingly. As these directions are considered to have the highest level of control, it is interesting to examine how the work is evaluated and followed up, and for this study, the content of information security work is examined. The central documents for the analysis are the appropriation directions and the corresponding annual reports for 2021 and 2022. The initial aim is to determine whether information security is mentioned in the appropriation directions. The annual reports for 2021 and 2022 will also be examined in detail to gain a better understanding of the evaluation and follow-up procedures. Annual reports are produced by government agencies, which account for the objectives and tasks they have completed in the previous year. In general, the annual report accounts for specific tasks that have been declared in the appropriation directions (ESV 2023). Therefore, if specific information security tasks are identified in the appropriation direction, these tasks and the overall information security work will be observed in the annual report. In some cases, assignments from the appropriation direction are included in specific reports submitted directly to the agency's ministry. It is therefore possible that some specific reports may also be included in the content analysis of public documents.

3.2.2 Selecting Informants

An additional data source is needed, as the analysis of appropriation directions alone will not suffice as evidence. At least ten informants will be selected to obtain a comprehensive view of information security evaluation and follow-up work. The sample for this study is considered self-selection sampling. It involves announcing the need for participants and then allowing individuals to choose whether to participate in a study (Saunders, Lewis and Thornhill 2017). As potential informants will be contacted by email asking them to participate, they will have the opportunity to accept, or decline based on the information they receive about the study. Sometimes, self-selection sampling can lead to selection bias (Berndt 2020). However, the method is convenient for the study as there are 39 government agencies of interest, and the desired informants are expected to work with information security in a similar way within the agencies.

The interviews' purpose is to broaden the picture and capture what the document analysis cannot. To better understand how evaluation and follow-up are carried out within the government agencies responsible for civil preparedness, most interviews will be conducted with informants from the agencies. It is also considered relevant to the study to obtain insights from informants who do not work within the agencies. Therefore, three informants will be selected who have

worked in leading positions with information security in both the public and private sectors for most of their careers. They will be referred to as "Senior Informants". The three informants aim to deepen the understanding of the problem area and why, in particular, evaluation and follow-up are challenging. Table 1 displays a compilation of the informants and a brief description of their roles.

Emails were sent to all 39 government agencies responsible for civil preparedness, asking if they would like to participate in the study. The email contained information about the study and its purpose. The emails were sent to the administrative office in the hope that they are forwarded to a person or department that deals with information security. In addition, as the study was conducted with the help of an information security company, some aid in finding informants was provided by employees of the company. That is, employees with potential contacts within some government agencies was able to assist in contacting the agencies.

Table 1. Compilation of informants and their roles

Informant	Role
1–7 Agency Informant	Working with information security within the government agency
8–10 Senior Informant	20+ years of experience with information security in public and private sector

3.3 Data Collection

Case studies often use multiple sources to collect data. For example, both quantitative and qualitative techniques may be combined. The combination of different data collection techniques is called data triangulation. This approach allows the problem to be observed from different perspectives, giving a holistic view of the phenomenon. It is also said to make it easier to confirm or question the findings. When data is collected using different techniques and the problem is viewed from different perspectives, some caution should be exercised in the observation, as it may cause some confusion if the perspectives show different results. Therefore, critical evaluation of the evidence is essential for the evidence to be meaningful. Further, it is argued that triangulation can increase the validity of the study, meaning that the appropriateness of the choice of method can be strengthened if the research question is thoroughly answered (Bell 2016; Crowe et al. 2011). Yin (2013) also argues that data triangulation can strengthen validity. The use of two data collection techniques for overlapping data can provide greater certainty in the evaluation of the result.

3.3.1 Collecting Public Documents

All appropriation letters are published and available on the website of the Swedish *National Financial Management Authority* (ESV). Since 2003, the appropriation letters are published electronically, so it is possible to find the directions from previous years. Something noteworthy is that appropriation directions are occasionally changed or updated during the year (ESV n.d.). For this study, the most recent version of each government agency's appropriation direction were used for document analysis, as it provided the highest consistency. As mentioned above, the appropriation directions of the 39 government agencies responsible

for civil preparedness were analysed. However, it should be noted that the appropriation direction for SÄPO is confidential, and only part of its funding is publicly available (SÄPO 2023b). Therefore, these directions were not included in the analysis. In addition, the Psychological Defence Agency was established on 1 January 2022 (Statskontoret 2023). Consequently, only the appropriation direction for 2022 was examined. Accordingly, the total number of appropriation directions for which data were collected and analysed is 75, as the analysis included a comparison of appropriation directions between the years 2021 and 2022. As mentioned above, the 2021 and 2022 annual reports of the 39 government agencies were also included in the data collection and analysis. The reports were available on each agency's website, making them easily accessible for data collection. However, the same criteria as above apply to SÄPO and the Psychological Defence Agency, thus their reports were not included, bringing the total number of annual reports to 75. Combined, the appropriation directions and annual reports result in a total of 150 reviewed public documents.

Table 2. Criteria list with keywords to use during data collection

#	Content	Keywords
1	Text that are to be collected should refer to the following topics:	Informationssäkerhet, cybersäkerhet, IT, säkerhetsskydd, digitalisering
2	Text that are to be collected should describe how the agency works with information security:	Utvärdering, uppföljning, ledning, styrning, kontroll, revision, utmaning, systematiskt, risk, uppgift, återrapportering, förbättringsarbete, kontinuerligt
3	Text that are to be collected should describe information security tools, and/or guidelines that the agency uses:	Informationssäkerhetspolicy, standard, ledningssystem, föreskrift

To make data collection efficient and to collect relevant data, a list of criteria was utilised, shown in Table 2 above. The list was based on the research question and the research background topics. As the author is also familiar with the layout of the public documents and has knowledge about common keywords in the documents, these keywords served as a foundation for the criteria list. The list was used during data collection to extract only content according to the criteria. The choice to write the keywords in Swedish was motivated by the fact that these are the actual words found in public documents. In addition, although terms such as "säkerhetsskydd" (protective security) and "digitalisering" (digitalisation) do not have the same connotation as information security, they were included as keywords because it is common in public documents for a headline to be named this way and for information security to be elaborated on below. Therefore, such headings needed examination not to miss any information security content.

3.3.2 Conducting Semi-Structured Interviews

Given the qualitative nature of the study, it is appropriate to choose a qualitative method for collecting interview data as well. Therefore, it is applicable to conduct semi-structured interviews as they are flexible and allow for supplementary questions (Patel and Davidson 2019). Unlike structured interviews, semi-structured interviews enable the researcher to follow up with questions tailored to the

specific informant rather than having a structured interview protocol that does not allow further questions (Leedy and Ormrod 2015). When developing the interview protocol, the questions can evolve around different themes and, if necessary, during interviews, certain questions related to the themes can be omitted if they are not deemed relevant (Saunders, Lewis and Thornhill 2017). Furthermore, semi-structured interviews are also beneficial because they allow informants to explain the topics as they wish. Thus, it is essential to let the informant talk about things that may not be explicitly related to the proposed question. It requires a thorough analysis afterward but is also necessary for obtaining important nuances (Bell 2016).

Although it is possible to modify the questions depending on the informant, two distinctive interview protocols were prepared for the semi-structured interviews. However, the topics were similar, but some questions specifically relate to how the government agencies work with the evaluation and follow-up of information security, so these questions were not as applicable to the senior informants. The themes and questions in the interview protocol were based on the research background to assure relevant questions. Furthermore, the protocols received feedback from the supervisors of the authors, hence some adoptions were made. Although the initial questions of the protocols involve the working background of the informants (see Appendix A and B), this information was not used in the analysis. Hence, the questions were mainly included to break the ice and, and for understanding their background within the public sector. Furthermore, the interview protocol was not sent out beforehand, as it could minimise the chances of getting spontaneous answers. Semi-structured interviews are beneficial because they are interactive, with the potential for new topics to emerge (Busetto, Wick and Gumbinger 2020). The informants received brief information about the four main topics of the interview, allowing them to assess whether they were the right individuals to answer the questions. As mentioned above, emails were sent to the 39 government agencies and the other potential informants. All interviews were conducted digitally using a video conferencing tool, which all informants were informed of during the initial email correspondence. The interviews did not exceed one hour, with each interview lasting approximately 45-60 minutes. Informants were also asked if they agreed to be audio recorded so that the author could transcribe the interviews afterward.

3.4 Data Analysis

Combining two methods for data collection provide a thorough understanding of the problem area, but also enables interpretation of the data that could result in seminal findings. Thus, the data analysis procedures are detailed below.

3.4.1 Qualitative Content Analysis of Public Documents

The qualitative content analysis was conducted on a total of 150 public documents, where the objective was to investigate whether evaluation and follow-up are performed and if specific information security assignments and objectives are reported from one year to another. The content analysis method is an exploratory process where both an inductive and a deductive approach can be used. Similarly, the analysis can be qualitative or quantitative (Stjernborg and Mattisson 2016). The appropriation directions include quantitative data, as the funding

is presented in them, but they also include specific assignments that the government agencies should report on. Similarly, most of the content in the annual reports is qualitative. Therefore, the content analysis was based on the criteria list explained above and focused on specific words and sentences that express meaning, which is also the focus of qualitative data (Saunders, Lewis and Thornhill 2017).

Stjernborg and Mattisson (2016) conducted a content analysis of public policy documents, focusing on the so-called manifest content, which refers to the content clearly expressed in texts. As the documents analysed in their study are reminiscent of appropriation directions and annual reports, the content analysis was performed similarly. The first step in the content analysis was to go through each of the 75 appropriation directions and extract relevant data according to the keywords in the list of criteria. The extracted data was entered into two tables, one for 2021 respectively 2022, with identical columns. An example of how the table looks like is shown in Table 3. The tables have five columns, the first of which indicates the government agency, its ministry, and the date of the decision. The second column explains what type of keyword has been identified, the third column contains extracted data about the information security assignment, requirement, or objective, the fourth column states to whom the assignment should be reported, and the last column contain other extracted information if necessary.

Table 3. Example table for extracting data from appropriation directions

Government Agency/Ministry	**Keyword**	**Assignment/Requirement/Objective**	**Report to who?**	**Other**
Government Agency: Ministry: Date of decision: 2021-xx-xx	Information security	The agency should comprehensively account for their information security work.	Annual Report 2022	-

When analysing the annual reports for 2021 and 2022, the assignments and, or requirements stated in respective appropriation direction were first identified and extracted in the annual reports. Thereafter, the criteria list was again utilised to identify all content related to information security and follow-up in the annual reports. The extracted data was put in a table listing the government agency, which document had been examined, the extracted content, and the coding. Below, Table 4 serves as an example of how the data extraction could look like.

Table 4. Example table for extracting data from the annual reports

Government Agency:	XX
Document:	Annual Report 2021
Content:	The agency works systematically with information security and has improved risk classification during the year. There is however work required to achieve an acceptable level of information security.
Coding:	Systematiskt, förbättringsarbete, kontinuerligt

Stjernborg and Mattisson (2016) point out that several readings are needed to understand and contextualise the extracted parts, it was also the case for the public documents. Subsequently, categories based on the coding were created describing how and to what extent information security is evaluated and followed up. It involved dividing the data into meaningful categories. The categories can emerge from the theoretical background (Saunders, Lewis and Thornhill 2017), but for this study, the research background together with the criteria list served as the basis for creating categories. An initial thought was that the follow-up procedures found could carried out in different ways, hence the research background was deemed a relevant source for deriving themes. As the themes in the research background are vast, it was assumed that the derived categories would need to be narrowed down to create meaning and allow for thematic coding and analysis. Consequently, it was performed, and suiting headlines for the result were derived based on the identified themes.

3.4.2 Qualitative Analysis of Semi-Structured Interviews

Saunders, Lewis and Thornhill (2017) recommend writing a summary after conducting an interview. It will capture any interpretations that arise during the interview. Writing down observations can be crucial if something happened during the interview that could affect the data collected. The notes can also be useful for later analysis of the transcribed material. As the interviews were audio-taped, the analysis of the semi-structured interviews begun with transcribing the interviews. It was done using Microsoft Word and the built-in transcription tool. The transcribed material was printed, making it available both electronically and physically. The first steps of coding can be easier when the data is physically available, and it is possible to make notes in the margins or underline certain things. Since there is a variation of ways to categorise and code data, it is preferable to do so in a way that best suits the purpose of the study and the type of data (Bell 2016). Therefore, the analysis procedure for the interviews was similar to the content analysis of public document. First, the transcribed material was read through and relevant findings were underlined. During the second reading, coding took place based on the list of criteria explained in Chapter 3.3.1. The research background also assisted in the coding. When completing the coding, categories were created, and content including similar findings were grouped. As a result, the material was divided into headings, with each category given a meaningful name, and the collected content accounted for.

3.5 Validity and Reliability

The researcher must be aware of certain threats to the validity of the choice of method (Berndtsson et al. 2008). The potential threats to the choices made for this study are therefore carefully considered. Research validity refers to the intentions of what to measure in the study and how well the study measures these intended aspects (Berndtsson et al. 2008). As there is little previous knowledge of evaluation and follow-up within Swedish government agencies, the choice of a qualitative case study with an inductive approach is appropriate. As mentioned earlier, one can argue that the research approach also has some deductive elements, as the content analysis will derive themes from the research background.

When conducting a case study, the researcher must, to some extent, understand the problem in advance. The researcher may also have chosen a case study to advocate certain issues (Yin 2009). Therefore, a common threat to the reliability of qualitative research is researcher bias. When conducting a case study in a particular organisation or setting, the researcher will go into the project with some preconceptions, and it is difficult to avoid this. Therefore, the researcher must report any bias and conduct the research with the highest degree of subjectivity (Berndtsson et al. 2008). There is a risk of bias when conducting interviews, as the interviewer may influence the participant without being aware of it, which could lead to bias in the data. A researcher with a vested interest in the phenomenon under study has a high risk of being biased. However, by being aware and considering all data with equal attention and not excluding anything, the risk is minimised (Bell 2016). To avoid such a bias in this study, the literature search for the research background is extensive in order not to miss any important aspects. Similarly, the analysis will be thorough and subjective to produce legitimate findings.

A qualitative interview is a good tool for collecting rich data (Myers and Newman 2007). For example, audio-taped interviews have the benefit that the interviewer does not have to manually document the interview. Instead, it is possible to listen to and interpret the responses. However, there are threats to the reliability of the method. If the participant knows that he or she is being recorded, there is a risk that they will be reluctant to be open and honest in their responses (Walsham 2006). As a result, important information may be omitted. Therefore, it is important to consider the interview setting where possible. As the interviews in this study were all conducted digitally, the circumstances were similar. However, if the researcher is nice and polite, but also fulfils the promises made to the participant, potential problems with the audio recording are limited (Bell 2016). Reliability could also be compromised if interviews are conducted with the same participant on different occasions. There is a possibility that the participant may have changed their perception of the topic, and the researcher could also change their perception if new insights are discovered during the conversation (Patel och Davidson 2019). As this study only conducted interviews with the participants on one occasion, the risk of the above was considered limited.

The selected public documents, that is, the appropriation directions and annual reports, are the final caveat to potential reliability issues. In general, intentional sources are documents originally published for purposes other than research. These may include government and official documents or protocols of various kinds. It is therefore crucial to consider that the author of such documents may have published them with a specific purpose in mind (Bell 2016). Appropriation directions are delivered by the Swedish government. Hence, they have a political agenda as they want to execute their politics. The annual reports are declared by each government agency, which reports to the Swedish government on the work they have undertaken. Thus, they must account for if they have not achieved any of their annual objectives. As the appropriation directions are documents with a political agenda, the researcher should be aware of this fact. However, as the appropriation directions and the annual reports are the only type of documents analysed, no further comparison with other types of documents were necessary, which also aided the analysis part, as they had the same structure.

3.6 Ethical Considerations

Most case studies deal with current human affairs, so ethical considerations are crucial (Yin 2009). There are four main ethical requirements that the researcher should consider. The first is that the researcher should inform the participants of the purpose of the study. The second is that participants should be aware that they can withdraw from the study at any time. The third is about confidentiality, where the researcher should ensure confidentiality for the participants, also personal information should be managed by authorised persons involved in the study. The fourth aspect is that information collected should only be used for the research (Patel och Davidson 2019). In this study, the above requirements were taken into account to ensure the safety of the participants. Firstly, the respondents who agreed to participate were informed about the purpose of the study via email before the interview, they were also encouraged to ask any further questions. Before the interview took place, the participant was given a consent form to sign, which stated that the participant could withdraw without consequence, that they were informed about the purpose of the study, and that they were guaranteed confidentiality. As the interviews were audio-taped, participants have been informed that the recordings will only be available to the researcher and that the material will be stored locally on the researcher's computer. Furthermore, the recordings will be deleted by 2023–07–31 at the latest. By providing this information, both participants and the researcher established a common understanding that increased the chances of productive interviews.

The informants from the participating government agencies will not be mentioned explicitly. The closest explanation is that they are among the 39 civil preparedness agencies. Similarly, the senior informants are not further identified. The motivation for this choice is that the study aims to ensure anonymity to the greatest extent possible. It is also thought that the quality of the interviews will be enhanced, as informants may be more willing to talk freely about the subject.

4. Results

This chapter presents the empirical data, starting with the results of the qualitative content analysis of public documents. The results obtained from the semi-structured interviews are presented in Chapter 4.2.

4.1 Public Documents

According to the criteria list and coding, the data were divided into categories where similar but also contrasting findings within the same theme are presented together. In total, 152 public documents have been analysed. Thus, two documents were added, namely “LM2021/053119” and ”Informationssäkerhet - Svar på regeringsuppdrag”, both being publicly available when searching for them online. These were added because the two agencies referred to them in their annual reports for 2021 regarding their work with information security. First, the appropriation directions are illustrated. Key figures derived from the extracted data are then presented. However, no agencies are explicitly mentioned as it is not relevant for the study to know which agency conducted what work. Therefore, the agencies are referred to as "one agency" to provide examples from the public documents.

4.1.1 Key Figures from Appropriation Directions

The appropriation directions have been examined and analysed to understand how information security is evaluated and followed up. The section begins with some figures derived from the appropriation directions. The figures themselves do not express how information security is evaluated and followed up, but they are important to consider because, together with the rest of the empirical data, they can assist in answering the research question.

For both years in the 2021 and 2022 appropriation directions, 18 out of 38 investigated government agencies for civil preparedness did not receive any reporting requirements or assignments regarding information security. In nearly all of these cases, the same agencies in both years did not receive any instructions. As a result, they were not required to report to the government on information security in the annual report. The reason for this may be that they had already received instructions in previous appropriation directions, or they have now received instructions for 2023. However, it is notable that some of the 18 government agencies have received brief instructions on how they perform their work concerning being an agency for civil preparedness. When reporting their work in the 2021 and 2022 annual reports, some agencies opted to include information security in their overall civil preparedness work, but most chose not to do so. In addition, it was found that three agencies had identical reporting requirements and assignments in both years. A commonly identified pattern is that an agency received no or short instructions in the 2021 directions. The instructions were then extended in the 2022 direction. Where there is an extension of a direction compared to 2021, it can be observed that the 2022 direction states that the agency should account for its information security work in some way. However, three agencies in 2021 and 12 agencies in 2022 received what is considered general or condensed instructions. General or condensed instructions vaguely describe what the agency should do concerning its information security work. Frequently used terms in this context are "comprehensive measures", and "information security must be taken into account in the work". Thus, the appropriation

directions do not explain *how* the agency should carry out its work, but rather what it must do and report on. When agencies are required to report, the majority of instructions in both years state that the account for information security should be "brief" and "concise". In addition, several instructions are identically worded, although they come from different ministries. However, it is not within the scope of this study to investigate whether the ministries have collaborated in any way to develop similar instructions for the appropriation directions.

15 agencies received an extension to their 2022 instructions compared to their 2021 instructions. Eleven of the 15 agencies had no instruction for 2021, while the rest had a brief instruction now including specific assignments or reporting requirements. In parallel with this finding, several agencies received their first specific information security reporting requirement in the 2021 direction. It was identified by the wording of the instruction. For example, phrases such as "actions that the agency plans to take" followed by "to ensure that the agency conducts systematic information security work" can be found in several 2021 directions. When these phrases are combined with the data extracted from the annual reports (which are accounted for later), it becomes clear that an agency has only recently started its information security work. When examining the corresponding appropriation directions for 2022, the wording has evolved as the agency has reported back on its 2021 work. For example, the developed wording now includes "the agency should account for whether action has been taken to manage identified risks". In addition, for the 2022 directions, the agency may also be asked to describe how it has worked to strengthen its information security work. One agency that did not receive information security instructions in its appropriation direction until 2022 discovered the need for measures earlier, as can be seen from the annual report for 2021. In the report, the Director General estimates that there were deficiencies in internal governance and control, and an internal report revealed that the information security work was not satisfactory concerning the MSB provisions and the *Infosäkkollen* survey. After receiving instructions in 2022, the same year's annual report states that the information security work is still in the development phase and that they perform follow-ups every six months according to MSBFS 2020:6. However, the same agency reports that they still do not meet the requirements, but they are continuously working on the issue, and the top management is aware of the situation and follows it up continuously. This agency is not the only one to express a demand for requirements before receiving instructions. However, the example highlights the need for governance and direction at an early stage before the work becomes challenging to resolve.

A calculation was also performed to see which ministry had produced the most detailed information security instructions in the appropriation directions. Each agency for civil preparedness works under one of the eight ministries in question. The number of government agencies under each ministry was calculated. Then each agency with its ministry was examined for 2021 and 2022 to see if it had any instruction in the direction and whether it specifically included information security. Based on the derived number of agencies with an instruction under each ministry, the number was calculated and is displayed below in Table 5 as a percentage. The motivation for presenting the figures as percentages were due to the ministries having a variety of agencies and it was therefore considered appropriate. For example, the Ministry of Employment has only one agency, while the

Ministry of Infrastructure has nine. In Table 5, zero in any of the columns indicates that the ministry did not distribute any information security instructions to its government agencies. If the number has increased in the 2022 column, it displays that government agencies have received an instruction, presumably for the first time. Or that the previous year's instruction was expanded to include more detailed instructions on information security. Where the numbers are the same, no instruction, or the same instruction was issued in both years. Accordingly, the table depicts that five out of eight ministries distributed or expanded information security instructions in the appropriation directions to government agencies in 2022 compared to 2021. For the other three, no information security instructions were identified in the appropriation directions for either year.

Table 5. Agencies with an information security instruction in their appropriation directions 2021 compared to 2022, presented in percentages

Ministry	**Number of Agencies**	**2021 (%)**	**2022 (%)**
Ministry of Employment	1	0	100
Ministry of Finance	6	0	50
Ministry of Infrastructure	9	11	33
Ministry of Justice	7 (2021) 8 (2022)	29	50
Ministry of the Environment	3	0	0
Ministry of Enterprise and Innovation	4	0	0
Ministry of Health and Social Affairs	6	17	83
Ministry of Education and Research	1	0	0

4.1.2 Half a Page is Enough

Generally, annual reports are between 80 and 150 pages long, although some are longer. However, as many appropriation directives clearly state that information security work should be kept short and concise in the annual reports, agencies do so. In some reports, information security has been given its own heading, in others it is mentioned together with overall security within the agency. Some have also combined information security reporting with IT work. A common feature of almost all annual reports with a dedicated information security heading is that the section is shorter than a page. Often it is about half a page. Hence, in a report of around 100 pages, there is not much focus on information security and the measures taken to improve it. Often agencies describe information security, why it is important in their organisation, and why it must be protected. Sometimes the formulations are almost identical, even though different agencies from different ministries have written them. When the section goes on to describe the actual information security work they have conducted, it is short and includes only a few measures taken. For example, it is common for these reports to say that they have provided education for employees, or that they have changed a policy document.

4.1.3 The Work is Ongoing

Examining the appropriation directions and linking them to the respective annual report provides a broader understanding of how information security is evaluated and followed up. A recurring factor is the ongoing nature of information security work within agencies. As mentioned above, it was noted that several agencies have recently started to work systematically on their information security, in addition to receiving instructions for the first or second time in their

appropriation directions. The annual reports provide an opportunity for agencies to be honest about the work they have undertaken during the year. Concerning information security, several reports describe the work as ongoing. Although measures have been taken to improve information security, several agencies describe that there is still a considerable amount of work to be done. Several appropriation directions state that an agency should report how it has systematically worked with information security during the year. In the annual report, agencies describe that they do work systematically, for example by carrying out risk analyses to identify critical risks. One agency mentions that it carried out such an analysis and then created the necessary activities to mitigate the risks. However, only 50% of the activities were implemented during the year and the remaining 50% are to be implemented in the next two years. Another agency expresses concerns about its information security work, as the shortcomings identified could lead to non-compliance with the Data Protection Regulation and other provisions related to information security. In addition, the agency states in the 2021 report that an evaluation of the current systematic information security work has been carried out and that the development of the work will continue in 2022. In the 2022 report, the work has been followed up and the information security work is now at a basic level, but not satisfactory, thus further work is required. The annual reports also show that some agencies have followed up on internal governance and control, and the evaluation has identified information security as an area for improvement. One agency has for several years identified information security as an area for improvement concerning internal governance and control. In addition, measures have been taken over several years, such as the implementation of an ISMS and the development of new governance documents. As a result, the agency has now assessed the area as compliant, but only regarding governance and control.

In addition, the work described in several reports for both years involves the development of internal procedures and guidelines. Although the agencies express the need to continue to work with them as they are not considered complete. While agencies describe measures taken, a common factor in the reports is that the measures are not explained in detail. In most cases, the measures involve decisions, plans, or developments. As several directives state that agencies should describe how they have planned to take measures, agencies are obliged to report on this work in the annual reports. However, there is no thorough description of how or for what they have planned. Additionally, several agencies have used the same wording in both years' reports to describe how they planned for information security during the year. As a result, it is sometimes not possible to clarify what has been done within the agency as no examples are provided. On the other hand, certain formulations in the appropriation directions are comprehensive but simultaneously ambiguous. In one appropriation direction it is stated that the agency should perform internal development by applying new working methods and digitalisation, in this work information security should be particularly accounted for. Though, no further explanation for which working methods to utilise is described.

4.1.4 Internal Audits and Follow-Up

The findings explicitly indicate that many agencies perform some type of evaluation and follow-up. However, it is challenging to observe how successful they are. The procedures can include internal and external audits. More than half of

the agencies report that they carry out audits, some do both, and others only one. In connection with the internal audits, follow-up is continuously performed. Sometimes the whole agency is followed up annually. Other agencies have chosen to follow up on specific parts of the organisation, such as specific projects related to information security. In 2021, one agency reports that it embarked on a project to implement an ISMS and to review the work, it was decided to carry out a systematic follow-up after seven or 12 months. To ensure that the implementation was underway, the follow-up procedures were to cover both projects and the entire organisation. However, the work started in 2020, but the agency states in its 2022 report that the implementation work has just now entered the management phase. Although several agencies have only recently started the process of developing an ISMS, several agencies report that they have implemented a functioning ISMS. Where this is the case, most of these agencies also report that they have based it on ISO/IEC 27001. Specifically, the management review is mentioned as one of the key activities for improving the ISMS. It is generally reported to be carried out on an annual basis or when new information security measures are implemented.

Follow-up based on EU regulations and directives is also mentioned. One agency mentions that it started ISMS implementation the previous year and continued it into the next. Examples of activities include the integration of policy documents into the agency's security department to support managers and staff. In connection with this work, a risk analysis was carried out, with one risk being that they would not be able to comply with MSBFS 2020:6. With continuous improvement work under the ISMS, they were able to state in the following annual report that the risk had been managed in accordance with the paragraph on how to follow up in MSBFS 2020:6. Although they maintained the risk, further action was required in relation to the overarching information security work. Despite the previous finding suggesting successful follow-up, other agencies report that the majority of identified and critical risks are related to information security, and many agencies report that such risks have existed for several years. For these cases, it is common for the reports to state that the risk and its mitigating activities are the same for both years and that work to minimise the risk continues. However, the agencies do not explain in detail how the mitigation work is carried out. Almost half of the agencies state in their annual reports that the follow-up and evaluation of information security is the area of improvement that requires the most attention.

Another way of following up and evaluating within several agencies is the MSB's *Infosäkkollen* survey. Some agencies describe in their reports that they have used the tool to gain knowledge about their information security level. The results are mixed, but the majority of those who have conducted *Infosäkkollen* report that the result of it is consistent with their internal analyses. Furthermore, those who have carried out *Infosäkkollen* also report that the overall information security is at least at a basic level or higher.

4.1.5 Responsibility is Challenging

The examples above demonstrate that agencies carry out follow-up and evaluation in different ways. The reports show that some are more successful than others. The instructions in the appropriation directions are vague and do not de-

scribe how information security work should be carried out. As a result, the annual reports show a variety of methods used by agencies to carry out their work. As noted above, standards are the preferred method for some, while others have opted for external audits. Nevertheless, they all have to carry out their work based on the principle of responsibility. It is therefore interesting to note that the agency mentioned above identified the need for information security before receiving an instruction. The annual reports show that the opposite is almost always the case - agencies do not prioritise information security work before they receive an instruction. As a result, as the reports show, several agencies have only recently started their information security work. One of the reasons for it can be deduced from the reports. Several agencies mention a lack of resources in the area of information security, including both funding and difficulties in recruiting the right competence. Consequently, some agencies report that they have been forced to postpone information security projects. For example, one agency that was supposed to perform information security supervision of other agencies was not able to perform any supervision during 2021, which they attributed to the pandemic and lack of resources. At the same time, it is interesting to note that they report challenges with their own information security work. They describe the work as ongoing and it will take several years to reach an acceptable level. The same applies to another supervisory agency, which states in its 2021 report that it has just established that it should be working according to an ISMS. The agency follows up on the work in the 2022 report and states that the work with the ISMS has received a lower priority due to the high demand for resources within other projects.

Several agencies indicate that work on information security is ongoing and progressing slowly. However, there are conflicting views when examining the reports. Some agencies argue that digitalisation in society as a whole, and consequently within agencies, is moving at a rapid pace. In combination, the security landscape is also constantly evolving. One agency expresses the need to talk about security in the context of digitalisation, arguing that it is not currently the case. According to the agency, the consequences are a large number of new tasks related to digitalisation, which require the relocation of resources. As a result, the security aspects that should be required are not prioritised. Other agencies also express that digitalisation forces them to complete projects and assignments quickly and security is repeatedly forgotten. One agency described how changes in the security landscape had made them force several implementations.

4.2 Interviews

The list of criteria was utilised to categorise the data similarly to the public documents. The transcription of the ten interviews resulted in 60 single-sided pages, which were analysed. As mentioned above, informants are not identified by the agency or organisation they represent. Informants from government agencies will be referred to as "Agency Informant" and given a number from 1–7 to distinguish them (according to the numbers received in Table 1). As for the other informants, they will be referred to as "Senior Informant" and given a number from 8–10 (also according to Table 1).

39 agencies were asked by e-mail to participate in an interview, and a few (less than five) agencies were contacted with the help of the company the author collaborates with. Ten agencies declined to be interviewed, citing a heavy workload

in the area of information security. Four agencies were initially contacted by email but ultimately did not respond further as to whether they would be able to participate. Five agencies replied after the data collection phase had been completed. For the other agencies, no response was received.

4.2.1 Evaluation – A Versatile Method

When asking the informants how they manage information security, answers are varied. Information security evaluation within agencies is described as performed differently. Agency Informant 1 explains that they have an ISMS based on ISO/IEC 27001. The main objective of the system is to ensure that it is continuously developed. The ISMS should also ensure that the whole organisation works according to the ISMS. To strengthen this way of working, coordinators have been appointed in various departments within the organisation and they work tactically with the ISMS. In addition, the ISMS is evaluated by performing various measurements. These include measurements of the ISMS itself, but also to see how it is practically implemented and utilised in the organisation. The measurements are compiled and, based on the results, actions are proposed to the top management of the agency. A similar working method is described by Agency Informant 5, who describes that the agency has been working systematically with information security for more than 20 years. Each department has a coordinator who spends 10-20% of their time on information security issues. They provide a great deal of support, particularly in the classification of information, but also in internal audits. In addition, the internal audit work has improved, and the informant describes that they have integrated information security into the continuous internal audit of the entire organisation. In conjunction, the agency has also appointed an external company to carry out external audits every three years. Although having appointed coordinators are similar for both agencies. Agency informant 1 further explains the measures taken to develop evaluation procedures, which involves an evaluation model which is completed every year. The model is based on the different areas of ISO/IEC 27001. Additionally, questions have been defined based on ISO/IEC 27002, where they have selected questions relevant to the organisation. These questions are then sent to the organisation to answer according to a maturity level ranging from zero to five. Zero indicates no maturity, and higher scores indicate that the work is systematic and proactive. The questions are quite detailed and include whether the information is classified and if continuous follow-up is performed. The informant states that the maturity model works well because departments are forced to assess their level of maturity numerically, rather than just answering yes or no to the questions. It gives the agency an overview and allows identification of where the work needs to be improved. The agency has decided that not all departments need to achieve the highest score in the model, but the ambition is to be at a basic level or above. The agency has also identified the importance of asking slightly different questions to different departments. For example, the physical security or IT departments are asked questions specific to their work. These questions do not apply to the whole organisation, and the approach balances the results. If there are departments in need of improvement, action is taken. Either top management is asked to do something, or the strategic information security department could derive a new governance document or the like. Because the maturity model is performed annually, they can closely monitor the work and place actions where they are required. The departments also receive solutions that fit their needs. Thus, the solutions are tailor-made.

The opposite was also identified among the agencies. Agency Informant 2 states that they are in the establishment phase regarding the information security area. During the last couple of years, the security department has grown and the number of employees has increased considerably. Owing to the construction phase, evaluation, and follow-up procedures have not been performed.

> "I would say that we do not have systematic follow-up in the way that we wish and we are not there yet." (Agency Informant 2)

However, the informant explains that follow-up obviously appears in specific projects and that they monitor security-related questions. Even so, follow-up occurs sporadically and spontaneously within the information security area. Furthermore, there is awareness of how information security work is performed within the agency, although a systematic approach is missing. In addition, requirements from the EU force them to work with internal audits, but ultimately they are not where they want to evaluate information security. Tracing whether requirements from supervisory agencies and the EU are fulfilled is described as a challenge by Agency Informant 6. For a long time, the agency has not been able to trace and follow up on received requirements. Newly added requirements connected to the security area are burdensome because of limited funding, and there is insufficient knowledge to identify the lack of competence. The information security area has been disregarded for a long time, and not until recently, the agency has realised that it needs to take action. The work has not only been forgotten, but certain areas have also been unknown. Thus, information security is described as being anonymous. There are no people with the knowledge to ask about information security issues, routines are lacking, and potentially useful cheat sheets do not exist. Employees working with information security have simply done so part-time; hence, they do not have the knowledge to answer questions from other employees. Consequently, no follow-up has been conducted. At present, top management is aware of the challenges and heavy work required. Accordingly, following up on information security is a prioritised area.

Agency Informant 4 describes that they perform different analyses according to the MSB provisions MSBFS 2020:6 and 2020:7. Also, different measurements and the MSB survey *Infosäkkollen* are used. Utilising *Infosäkkollen* is relevant because MSB has well-established questions and measurements that the organisation can use. It is also interesting to compare with other agencies. Although they cannot see the results of specific agencies, comparing maturity levels is possible. The internal auditor also performs analyses of the ISMS, but the agency would like to increase the number of internal analyses. They have not been able to do as much as they would like due to a lack of personnel. Senior Informant 9 agrees that comparison with other government agencies is a good thing, and has also worked with incorporating information security benchmarking in the public sector. However, there is some hesitation about the *Infosäkkollen* because it is a self-assessment tool. There is hesitation because no supervision occurs based on the result. According to Senior Informant 10, there is a risk that agencies will overestimate themselves in the *Infosäkkollen*. However, the risk is not considered high because agencies want to show shortcomings in the information security work to receive support. Agency informant 1 has a positive attitude towards *Infosäkkollen* and also mentions the positive effects of comparison with other

agencies. It is particularly important for those who work with information security daily, as the survey provides insight into whether their work has an effect on the organisation. Still, the importance of creating evaluation processes that fit an organisation is crucial. Therefore, caution should be exercised when making comparisons, as each agency must choose a working method for evaluation that is the most suitable for them.

4.2.2 The Information Security Governance and Control – Does it Exist?

According to Senior Informant 10, the existing decentralised governance in the Swedish public sector can pose risks. Agencies are told to work systematically on information security, they do all sorts of analyses and must then manage these risks themselves. Thus, the agencies must develop their own measures, as the governing side does not explain how to do it. When asked whether anything is missing in the Swedish government's governance and control of information security, Senior Informant 8 says "plenty". The different perspectives of information security and cybersecurity are not fully understood by the Government Offices civil servants. Those writing regulations and provisions do not have the deep experienced knowledge regarding information- and cybersecurity required to formulate governance that can solve the issues. Some fundamental things related to information security should not be optional for government agencies, although it should be mandatory for all of them. In addition, information security and cybersecurity do not have a dedicated ministry responsible for the issues, which is the basis of the governance problem. Senior Informant 9 agrees that governance has been too weak, the requirement that government agencies must follow provisions has not been clear enough. With no requirements formulated from the government side, information security work is lacking. Also, the principle of responsibility has been used by the government, hence managers of the government agencies have been forced to take their own measures.

By contrast, several agency informants do not suggest that anything is missing regarding governance and control. Agency Informant 3 expresses a positive attitude towards the fact that *Infosäkkollen* has become mandatory for some agencies. As it now is stated in their appropriation directions they should report on their information security work. Formulating such requirements increases the prioritisation of information security issues. Agency Informant 4 states that governance is noticed in the different assignments and projects the agency receives in its instruction and appropriation directions but does not articulate whether something is missing. Agency Informant 1 does not wish for further governance and believes that the appropriation directions are sufficient and that MSB does a good job of developing different tools for support and evaluation. Agency Informant 2 also says there is a high level of support from their management and that is sufficient. However, two agency informants suggest that there is room for development in terms of governance and control.

> "We are touched by a lot via MSB, so what actually comes from the government, well, it is not that clear actually." (Agency Informant 5)

Agency Informant 5 discusses the fact that the government appoints the MSB to manage several tasks, which means that most governance comes from the MSB and other supervisory agencies rather than from the government itself. There are

also some elaborations on different ministries. According to the informant, the level of governance depends on the agency's ministry. The agency has recently moved from one ministry to another, and the security priority has turned out to be low; therefore, the focus is almost exclusively on the core business of the ministry. The informant has also noticed the differences in instructions in the appropriation directions depending on the agency, where some have received instructions and others have not. Thus, it would be reasonable to at least harmonise the appropriation directions between ministries in terms of how the agencies are governed. Therefore, according to the informant, more work needs to be conducted. Agency Informant 6 also suggests that governance could be developed, primarily by simplifying it. There are many regulations, provisions, and standards with which to comply, as well as supervisory agencies that oversee the work of other agencies. With so many regulations to follow, it is a challenge to do the desired work. The informant further explains that some government controls contradict other government controls. For example, functional controls and availability controls do not align with security regulations, which must also be complied with. Consequently, the agency is forced to compromise. In addition, the informant argues that there are now too many standards to follow and they are perceived as too wordy. Instead, each agency should receive simpler instructions on how to comply with regulations and standards.

There are differing opinions on whether the current governance methods, supporting tools, and guidelines are sufficient, or whether they should be extended. Utilising appropriation directions as a governance method for information security is inadequate. Governance should have been stricter and more measures should have been taken, argues Senior Informant 8. Furthermore, tools or guidelines for agencies could increase, but the problem is not that they are few. The problem is that very few actually are implementing enough security measures. In 2009, provisions for government agencies regarding information security were established, but these are still not followed. It is probably due to shortages in governance from the government. Senior Informant 9 discusses whether it would be appropriate to include information security requirements in the agency instructions rather than in the appropriation directions. Because many assignments in the appropriation directions are only temporary, it might be better to make information security a permanent assignment. The informant agrees with Senior Informant 8 on the compliance problem. Hence there should be sanctions incorporated into the requirements, otherwise, they are not met. Agency informant 6 also believes that appropriation directions do not help in practical work because they are formulated at a high level, similar to policy documents. Thus, they only declare areas that should receive attention and indicate that the agency should take responsibility for performing the assignments. In addition, there are a large number of tools and guidelines, but what is to be achieved with them, asks the informant. The tools and guidelines provided by various supervisory agencies are lengthy, and describe the importance of managing information security issues. However, there is a shortage of explaining how to implement them in practice, so there is a desire for more such guidance.

Agency Informant 7 believes the number of tools and guidelines is sufficient, although MSBs should receive more resources to develop them further. Moreover, Agency Informant 1 thinks the instructions they have received in their appropriation directions are enough because they use multiple methods to conduct and

evaluate their work. Agency Informant 3 believes the instructions in the appropriation directions are relevant. This opinion is supported by Agency Informant 4, who also emphasises that the work is not optional, but must be conducted. However, the informant believes that there can never be too many tools, but the agency already has many requirements from supervisory agencies and other regulations, therefore it is not necessary to add any. In other words, increasing the number of requirements does not guarantee that operations will become more secure. Instead, there is a desire for more tools in the form of resources, knowledge, or increased coordination between agencies. Agency Informant 2 describes that the agency has a clear direction in its information security work, so the appropriation directions are sufficient. Although they are in the construction phase of their information security operations, they do not require clearer governance. The current tools from MSB are good, but they are not used daily. The reason is that they are already affected by provisions from supervisory agencies, so these requirements are daily prioritised and worked accordingly. However, there is an expectation regarding the National Centre for Cybersecurity, as it will be interesting to see what kind of support it will be capable of providing.

4.2.3 Challenges with Follow-Up and Evaluation

To systematically conduct information security, the Plan Do Check Act (PDCA) cycle should be followed. Similarly, in the Method Support by MSB, the "Follow Up and Improve" phase is the last activity to perform. Senior Informant 10 believes organisations have a hard time reaching the final activity because they have completed several activities involving developing documents and implementing security measures. The first three activities require much effort, making it difficult to reach the final stage where they can start evaluating and improving the work. Instead, it is not necessary to finish all the work in the previous stages before moving on to the final stage. For example, the establishment of follow-up routines can be performed in the earlier stages, even if all other activities have not been completed. If the agency has a somewhat established ISMS, it is possible to create the basic requirements for performing follow-up and evaluation. One of the key activities to be carried out is the management review, which is used for showing the management how the work is progressing. Also, in the first year of the ISMS implementation, the results may not be excellent. It could be a good thing to lower expectations, rather the establishment of routines and processes is the most important, and then they will have the ability to improve during the next year. Equally, Agency Informant 3 describes the tendency to develop, analyse, and implement measures all at once because there is a willingness to complete them quickly. By the time the evaluation phase is reached, exhaustion sets in, along with the organisation perhaps not being on board with the changes. Senior Informant 9 shares the above view that evaluation and follow-up are difficult and often overlooked in the PDCA cycle. There are heaps of planning, but follow-up is not performed. In addition, the informant has experienced challenges in adjusting and auditing internal guidelines. Firstly, the guidelines should not be too extensive, although they should provide guidance "so that you can use your own brain to understand what needs to be done". Secondly, guidelines are not regularly audited, which makes them outdated. Then they also lose their function as a management tool because management cannot explain to the organisation what to do if they are out of date.

Furthermore, having an implemented ISMS without incorporating it into the regular management system of the agency will not allow for evaluation and follow-up, according to Senior Informant 8. The system should also connect to the overall IT governance and objectives of the organisation. For example, a measure equivalent to Key Performance Indicator (KPI) could be used within the public sector to develop plans and make decisions accordingly. Getting the attention of top management is also a challenge. People with the role of CISO or Security Officer must possess the capability to explain to top management what is required. It can be a challenge to motivate, but by providing top management with accurate information, they can make adequate decisions and take action to improve information security. The CISO or equivalent therefore needs to have the skills to motivate them and not merely beg for funding. Agency Informant 5 also recognises the importance of being pedagogical when explaining analysis results to top management. It is described as a constant challenge when top management does not prioritise taking security measures against identified risks. It is therefore crucial to explain that the risks could lead to certain consequences and to ask whether they are willing to take that risk. For example, it is natural to follow the economic aspects of an organisation, but information security is still a relatively new area to consider and has not yet received the attention it deserves. Also, when incidents occur, they always affect someone else, and it is not until it affects your organisation that it receives attention. Senior Informant 10 adds that the support of senior management is also crucial because of its symbolic value to the organisation. Not only do they have the ability to allocate resources and strategic roles, but supportive management leads by example, and many soft values at play are crucial to the success of information security work.

Certain activities should be performed as part of systematic information security work, but opinions differ as to which are the most challenging. The evaluation of security measures and the evaluation of internal rules, working methods, and support to make sure they are utilised appropriately is considered the most challenging by Agency Informants 3 and 4 and Senior Informant 10. These activities are challenging because evaluation is difficult and it is complicated to find systematic ways of doing it. It is also considered complex and requires resources, which could also make it time-consuming. Therefore, as mentioned above, it might be relevant to start the evaluation process earlier, even if other activities are not yet completed. Getting an evaluation result earlier could uncover shortages that must be managed. It could also increase the chances of speeding up the improvement process. Agency informants 2, 5, and 7 disagree and argue that information classification is the most challenging. Employees find it difficult to classify information according to the proposed method. Therefore, much time is spent on developing an understanding of it. Furthermore, there are large amounts of information to classify and both agencies and private actors working with the agencies perform classification in various ways. Therefore, Agency Informant 5 suggests that the government should focus on taking action and establishing a consistent method for classifying information. A centre similar to the National Centre for Cybersecurity, but focusing solely on information security, would be relevant, including a central point for how information classification is performed. The current focus is on security measures, but if agencies do not have knowledge of what assets to guard, it is difficult to protect what is worth protecting. On the other hand, Agency Informant 1 does not experience challenges with

information classification. When the agency follows up on information classification, there is a requirement to include several examples of information classification. It allows the agency to see that the activity has been performed.

> "If you then, as you should naturally have, x number of security requirements, which you also have to implement, and when they have not been taken care of for many years, it is a very high threshold to cross. So we have an awfully long way to go. Partly by implementing, and managing, to get it operating in the systems." (Agency Informant 6)

Furthermore, Agency Informant 6 believes risk assessments are challenging because the current environment focuses on ticking boxes. As a result, assessments may be considered complete when in fact they were conducted ten years ago and have not since been updated. As a result, it is difficult to evaluate whether risk assessments comply with current legislation.

4.2.4 Balance, Interpretations and Value

Finding a balance between conducting a compatible amount of evaluation and fulfilling the agency's core tasks is a challenge. The agency must not be overburdened with evaluation and follow-up tasks. At the same time, hardly any tasks are not a sustainable solution either, says Agency Informant 1. Similarly, Agency Informant 4 agrees that there must be a balance between requirements and the agency's capacity to produce and that working only on security issues is not plausible. A similar point is made by Agency Informant 5, who discusses that ministries should consider to a higher degree that the agencies are responsible for civil preparedness. There is a lack of prioritisation on the part of the ministries because they assign tasks to the agencies without any prioritisation, suggesting all of them are equally important. It is therefore up to the agencies themselves to set priorities and decide which tasks should be given more or less attention. The dialogue between ministries and agencies, therefore, needs to be improved.

There are also different perspectives on what should be included in information security. Agency Informant 5 describes that they have worked within the agency to distinguish information security from IT security because IT security has grown. In addition, cybersecurity has been in the spotlight in recent years. Senior Informant 9 agrees that there is confusion about the terms. It is motivated by the fact that cybersecurity sounds cooler compared to information security, which is about managing information, and IT security, which is about digitalisation. In addition, the Protective Security Regulation has received much attention recently, and agencies have made different interpretations about whether they are affected by it. Senior Informants 7 and 8 acknowledge this phenomenon, which means that pure information security and cybersecurity issues could be forgotten, even though information security has to some extent been incorporated into protective security. If agencies have different requirements, there is also a risk that different reports should be accounted for concurrently. Thus, agencies are forced to generate distinct results for different requirements, with the risk that less important requirements receive less prioritisation in the reports, as discussed by Agency Informant 3. As for requirements, Agency Informant 5 also points out that requirements can be interpreted differently depending on

whether there is an internal or external auditor following up on information security in the agency. Therefore, a future challenge is to ensure that both internal and, in particular, external auditors have a good knowledge of the upcoming regulations to find a balance when interpreting them. Furthermore, Agency Informant 1 argues that it is impossible to compare and evaluate all aspects of information security, so an efficient way of measuring would be relevant. As there are many regulations, rules, and standards to comply with, measurements are performed variously. Having a somewhat uniform method would allow for actions against focus areas.

Evaluating and following up on information security is not recognised as a value-creating activity in the organisation. According to Agency Informant 4, evaluation and follow-up are lagging because the agency assumes tasks are already complete. As activities must be performed continuously, it is considered a redundant effort rather than creating the desired value. It also consumes time and resources, and if the evaluation result is at a reasonable level, it is a challenge to motivate the agency as to why it is being performed. Therefore, the agency works hard to highlight the fact that the level of security will decrease if there is no evaluation and follow-up, and also to show that the work undertaken has added value since the results are positive.

> "[...] so there will be some kind of destructive hunt for crowns and pennies, which I think is devastating for the security work, because it is not really about saving money, but about preventing bad things from happening." (Senior Informant 9)

Senior Informant 9 does not believe that the results of investments in information security should be measured similarly to economics. It is because information security should not be considered solely a cost, but rather an investment in the entire organisation. It should be treated as something that improves the overall operation, instead, it is seen as a necessity to avoid being affected by disruptions. Similarly, decisions made by top management are generally focused on the strategic business values of the agency or organisation. As a result, decisions are often not aligned with security work. Similarly, security is placed under the IT budget, and IT officers are often rewarded for keeping to the budget, so no additional expenditure is allocated to information security. Instead, Agency Informant 7 argues that information security should be presented in a positive light because today it is negatively associated with problems and obstacles. Therefore, it would be beneficial to use the right rhetoric and associate information security with benefits that actors can gain from the agency.

4.2.5 The Relevance of Getting a Certification

On the question of whether an ISO/IEC 27001 certification would be relevant for the agencies, opinions disagree. Informant 6's agency follows ISO/IEC 27001 and 27002 but is not certified. However, the informant describes the standards as generic, which forces the agency to adapt accordingly. The standards are not considered to be directly tailored to the specific agency, as they manage several legacy systems that do not meet certain security requirements, making it difficult to achieve certification. Much work would be required to achieve certification as the agency does not currently have all the security functionality in place. Agency Informant 4 does not see certification as a security solution, but the maintenance

and follow-up of the ISMS are crucial. For the agency, certification would be relevant in terms of being able to display it as a symbol of quality to the stakeholders they work with.

Agency informant 5 is positive about certification, as they have quality and environmental certifications. Together with the internal auditor, information security is increasingly included in this audit. The informant would need more resources if it were to be certified but thinks it would be interesting if all agencies were certified, as this would give MSB a standardised way of observing the level of information security in each agency. Senior Informant 9 has a similar reasoning, that certification would provide comparable material. At the same time, it is peculiar that several agencies want to be able to certify but never get around to it. The informant experienced an increase in the maturity level of information security during their time in an organisation. Also, awareness of top management and employees increased, as they were interviewed by the auditors. With certification, external audits are performed annually and there is no way to hide things that are not working. However, there is a compliance risk, as some organisations want certification just to tick the box. At the same time, the informant argues that several current regulations have a similar compliance focus, so the risk of taking the easy way out in this area is just as great. Senior Informant 10 has witnessed positive changes in organisations that have been certified. It is because they are required to go through the whole PDCA cycle and establish systematic work. In addition, the organisation has to be capable of showing the auditors how it really works, so certification is a relevant incentive.

> "An ISO 27000 certification is a compliance measure that does not always lead to actual safety." (Senior Informant 8)

Senior Informant 8 develops the argument by saying that their opinion has changed slightly over the years. But the main point is that an agency should start with an ISMS and then implement at least three or four significant security measures to address critical risks. Hence, is more important than achieving certification. Agency Informant 3 does not think that ISO certification is necessary and should not be mandatory for all agencies. The standard contains relevant activities for improving information security, but the certification itself is not so important that it should be a requirement. Similarly, Agency Informant 2 believes that the journey toward certification is fundamental. Being able to present a certification is not important, but the involvement of the agency is crucial to improve the systematic work on information security. However, several other requirements demand the agency to improve, therefore certification is not the main driver. Agency Informant 1 says it is important to work according to the methods that suit the agency. Agency Informant 7 supports this view by arguing that if not everyone is comfortable working against a standard, then other methods should be used. However, the informant is in favour of certification as it would force the agency to continually improve the level of information security to maintain certification. It is not plausible that the agency itself would take the initiative to become certified, but a requirement from the EU or similar could bring about significant change.

4.2.6 Increased or Clearer Requirements?

At present, several agencies are affected by different regulations and provisions. The NIS2 directive is being transposed into Swedish law and other regulations are on their way. The informants describe the positive and negative aspects of the increased number of regulations and requirements. Agency Informant 5 describes an uncertainty about whether the NIS2 directive will affect the agency. In addition, the informant is positive about it because it will hopefully clarify the work required internally in the agency. In addition, directives and regulations involving sanctions are necessary because otherwise, it is too easy to prioritise other assignments. Agency Informant 4 is also unsure whether the agency will be affected by NIS2. Both Agency Informant 4 and Senior Informant 10 have a positive attitude towards the directive because it is an EU directive that could improve information security and cybersecurity resilience within the union. Furthermore, it will also create stricter requirements for top management, which will contribute focus to the area. It would also be positive if the MSB's mandate were extended, as security issues would be increasingly prioritised by top management. In addition, the current situation calls for stricter requirements and supervision.

> "[...] I believe the view is similar in other agencies and organisations, although not all. We are very, very few who work with security. This means that we have a limited opportunity to provide the support that the business deserves." (Agency Informant 4)

Senior Informant 9 believes that sanctions could improve evaluation and follow-up, but that the implementation of the NIS2 directive is taking too long. The informant argues that the current situation is poor and that changes take too long to implement. Furthermore, it would be relevant if, for example, MSB or a supervisory agency were given an extended mandate to supervise other agencies. Though, it would need to be equipped with the appropriate tools to make a difference. Agency Informant 3 believes that the NIS2 directive will involve additional work, as several organisations will be affected by the changes in the directive's requirements. A plausible consequence is that incident reporting will increase, as will the volume of information. Accordingly, Agency Informant 2 does not consider it necessary for MSB or other agencies to be given an extended mandate. The current provisions and regulations are sufficient, further governance would create additional challenges for both the supervisory agencies and the agencies affected. However, any kind of regulation similar to NIS2 is positive. For Agency Informant 1, the current situation is satisfactory. No further supervision by other agencies is needed. A provision or regulation where sanctions are included does not receive higher priority, because the agency strives to fulfil them all equally well. There would be no harm in extending the rules, but the current situation is working well.

Senior Informant 8 is not convinced that the NIS2 will affect the work of government agencies compared to the current situation. The informant also questions whether it is relevant that sanctions imposed on agencies are paid with taxpayers' money. Nevertheless, a stronger mandate for one agency and a clearer legal framework would probably increase the clarity of the regulations, instead of several actors issuing regulations. Agency Informant 6 believes EU directives make the consequences of non-compliance clearer. The fact that sanctions are required

is a pity, "if MSB gets a bit angry, well that's nice, but it does not happen, so the consequence is quite mediocre in that sense". GDPR and other regulations have clearly stated that if they are not followed, there will be a cost. In addition, if MSB were to receive an expanded mandate, they would also have to provide support in implementing the regulations. Currently, agencies receive all these regulations, but it is also their responsibility to interpret the regulations. Hence, the agency issuing the regulations must also aid in that work.

5. Discussion

This section first discusses the results identified in relation to the research background. It is followed by discussion around the ethical and societal aspects of the study. Lastly, limitations and future work are presented.

5.1 Previous Research

The term information security has received different definitions over the years (Horne, Ahmand and Maynard 2016). It has to some extent led to confusion about what to include in the domain. From the results of the annual reports, one can observe that there is no consistent way of interpreting information security. Some agencies have given information security its own sections, while others include it in IT security or digitalisation. There is limited uniformity in what to include in information security, with some agencies focusing more on cybersecurity or protective security. However, the interview results suggest that when working systematically with information security, it is crucial to recognise it as a separate area, even though it affects almost the entire organisation. It is not clear from the results whether the confusion around the term has harmed the ability to work with information security, but it does not appear to have had a positive effect either. Nonetheless, having a unified meaning for terms included in information security is positive according to Paananen, Lapke and Siponen (2020), who argue for an undivided approach regarding the information security policy. There is confusion not only about how to define the term but also about what activities should be performed in systematic information security work. The results of the content analysis and interviews revealed that it is difficult to simply tick the information security box. As a systematic way of working involves performing in cycles with continuous improvement, several interviews indicate that agencies struggle to assess when the work has been achieved. In addition, appropriation directions and annual reports illustrate that the same tasks are accounted for in both 2021 and 2022, suggesting that the work is not complete. Agencies also acknowledge there is a significant amount of work to be undertaken. Ghahramani, Yasdanmehr, Chen and Wang (2022) argue that organisations have a shortage of motivation to continuously improve the management of security, but they could not find out why. The results of this study suggest that it could be because several demanding activities must be performed in the cycle. Therefore, not all agencies possess the capability to complete the cycle because they reach a kind of exhaustion before reaching the final steps. Simultaneously, the activities have been rapidly performed, which does not guarantee that the organisation has been on board with the changes. Thus, the result indicates that the above method is not suitable for systematically establishing information security. As the interview result also indicates, there is an alternative way, where it is applicable to establish some routines early in the cycle, even though other activities are not complete. It allows for evaluation and follow-up, even though the results may not be favourable, although the organisation will have something to work with. This approach is supported by Broderick (2006), who argues that an organisation should agree on a minimum set of requirements associated with the ISMS that should be fulfilled, rather than rushing through several activities.

Information security should be briefly accounted for in the annual reports according to several appropriation directions. It could indicate a low priority for

information security compared to other tasks performed by an agency. Nevertheless, the fact that information security becomes increasingly included in appropriation directions also shows that the area receives deserved attention from the government. However, the result also implies that the government officials formulating the appropriation direction assignments may not have adequate knowledge of which aspects are critical to follow up. To define relevant regulations, it is crucial to have professional experience in the field of information security to understand all aspects of it. In addition, the absence of a ministry responsible for information security means that expertise is not concentrated in one place, and uniform requirements are not developed. It is possible to consider the appropriation directions as similar to policy documents, as both are high-level documents including the most important aspects of information security work. Therefore, one can assume that the suggested improvements to the policy could also be applied to appropriation directions and other information security regulations. Success factors in the implementation of an information security policy are the involvement of employees by raising the issues they identify (Stahl, Doherty and Shaw 2012). Also, making it useful is crucial for its success (Karlsson, Hedström and Goldkuhl 2017). The result of this study is blended, but there are indications that the appropriation directions are not an adequate tool for the governance of the agencies. Since the tasks in the appropriation directions are regularly exchanged, one result suggests that the instruction to the agency would be a suitable place to put information security requirements, making it a constant point. In addition, based on previous research, it may be relevant to involve agencies when drafting appropriation direction requirements to improve understanding of how the work is to be performed.

In addition to the fact that appropriation directions may not be suitable for regulating information security, there are also issues with ambiguous requirements. As mentioned above, appropriation directions are high-level documents and, not to forget, the utmost tool for the government to control agencies (Post- och telestyrelsen 2022). Therefore, the solution is perhaps not to include additional requirements in them. However, as there are no additional specifications on how to carry out evaluation and follow-up of information security, they must be included in the provisions and regulations for the work to be executed. As a result, it becomes burdensome because there are regulations, standards, requirements, guidelines, and supervisory agencies demanding requirements. As requirements are proposed by different actors, their intentions are unclear, the result tells. The National Strategy for Information Security and Cybersecurity states that the approach to information security should be unified (Regeringen 2023b). However, the agencies work under the principle of responsibility, which forces them to make decisions and prioritise work themselves. Åhlfeldt et al. (2018) highlight the importance of assigning responsibility when organising information security. As the results show, it is not currently performed in the suggested way, as several agencies ask for extended support on how to perform follow-up and evaluation. The results of both the content analysis and the interviews show that agencies use different evaluation methods that suit them best. However, there are some common methods, such as the *Infosäkkollen*, which most of the studied agencies have carried out and found supportive. Concerning *Infosäkkollen*, there are indications that agencies like the possibility of benchmarking against each other, although they do not explicitly know the results of other agencies. Thus, it is likely that benchmarking can serve as a motivation to improve evaluation and

follow-up. There is currently some information security cooperation between agencies, such as SAMFI (Informationssäkerhet.se 2015). As Ödlund (2007) also points out the benefit of inter-organisational cooperation between government agencies, possibly, extended cooperation could improve evaluation and follow-up among agencies if decision-makers create the right conditions. Including benchmarking in this collaboration could be beneficial, as the results show that agencies demand support in carrying out evaluations. Since cooperation is regarded beneficial by previous research, assumingly joint benchmarking would also benefit. In addition, given that most of the support for information security evaluation and follow-up is currently provided by MSB, the creation of this collaboration could presumably reduce pressure on MSB. As some informants express that MSB should be allocated increasing resources to improve their work even more.

Digitalisation seems to be a subject on which it is challenging to give an absolute answer. The result suggests that it is moving slowly, but also rapidly. The digitalisation in society is progressing, and some agencies are moving in parallel. Concurrently, the threat landscape is moving just as fast, and it means that digitalisation now equals an increased risk of cyber threats (IVA 2022). On the other hand, some agencies are also struggling with the rapid pace, as not only security measures need to be implemented, but also everyday activities must be performed. Similarly, the PDCA cycle security activities are extensive and should not be rushed, but they are. As a result, evaluation and follow-up activities are neglected because there is neither time nor resources to complete them. The research by Szczepaniuk et al. (2020) revealed similar results by arguing that the public sector has a key role in digitalisation development. However, their research also found that the public institutions in Poland had similarities to Sweden, with reviews, audits, and security controls missing. Thus, rushing digitalisation efforts may be a risk. It was mentioned in the result of the annual reports that security issues related to digitalisation are not announced. This phenomenon is a potential risk, as the government does not seem to acknowledge this fact. At the same time, rushing into digitalisation in the absence of adequate and systematic information security might result in agencies never catching up with the current deficit in information security and follow-up. Likewise, Jonathan (2020) argues that since IT investments in the public sector are based on political decisions, the top management does not always have the ability to make informed decisions. Furthermore, Justesen and Glerup (2018) claim that digitalisation efforts in the public sector cannot merely involve technological aspects, but must include developing working methods and strategies, thus digitalisation is a constant reform, and not a measurable objective.

The result shows that it could be relevant for government agencies to achieve ISO/IEC 27001 certification. However, it is not a consistent finding and some informants express that certification does not guarantee that security measures have been taken, as there is a risk that an organisation may solely want to tick the box. This view is supported in research by Boehmer (2008), who argues that an ISMS implementation based on ISO/IEC 27001 does not ensure quality and performance results are generated from the standard. ISO (2018) describes the ISO/IEC 27001 standard as broad enough to fit all organisations. However, one informant mentioned challenges with the standard due to its generality. Due to legacy systems, the agency struggles to meet certain security requirements in the

standard. Previous research supports this finding, with Siponen and Willison (2009) claiming that a number of the standards studied were too general to take account of organisational differences. As such, the security measures were also too general, with the result that no measures were implemented due to the generality. As mentioned earlier in the results, agencies have challenges in reaching the final stages of systematic information security work, which includes evaluation and follow-up. These activities are also among the last to perform in the ISO/IEC 27001 standard. According to the result, several agencies are working according to the standard, but most are not ready to achieve certification because some requirements are not fulfilled. As the result describes the evaluation procedures within the agencies as the most challenging part of systematic information security work, it can be assumed that these challenges may be a contributing factor in agencies not proceeding with certification. Ganji, Kalloniatis and Mouratidis and Malekshahi Gheytassi (2019) assert that ISO/IEC 27001 does not suggest how to meet the standard requirements. Their research supports the result of this study as, in particular, internal audit, management review, and continuous improvement lack recommendations on how to implement them. Thus again evaluation and follow-up aspects are not given attention. The authors also highlight the need for further research with how to meet the above requirements for follow-up. Also Lenning and Gremyr (2021) ask for further aspects connected to how organisations can improve and achieve their desired information security work. Presumably, extended recommendations on how to complete the systematic information security cycle could improve procedures.

Systematic information security is about continuously improving the work of an agency or organisation. The most important parts are evaluation and follow-up. However, as the result shows, the current focus of information security is on the various regulations and requirements that must be fulfilled. Accordingly, information security is perceived as an obstacle and a cost. Instead, as one informant describes in the result, the positive parts of information security should be highlighted. For example, emphasising the benefits of performing continuous evaluation and that having a functioning ISMS could positively impact the whole organisation. By promoting the positive aspects of information security, it might also be possible to change the view of information security as a cost to one of investment. It would then be easier to receive allocated funding for information security from top management. Research also indicates that top management's view of information security as a strategic issue is a success factor (Hedström, Kolkowska, Karlsson and Allen 2011; Posthumus and von Solms 2004). Despite Meyherhoff Nielsen (2019) investigating the Danish e-government strategy, the result showed that the success factors included well-aligned strategies and objectives across all government departments. On the contrary, current strategies for evaluating and following up on information security within Swedish government agencies are unclear and not well aligned between different ministries, the result tells. Therefore, more structured governance and objectives that do not interfere with the regular operations of the agencies are potential suggestions for improvement.

5.2 Ethical Aspects

One could argue that the study covers a somewhat delicate area. Previous research and the results of this study indicate challenges with the evaluation and follow-up of information security within government agencies. As the result also

expresses, the included agencies are aware that there is work to be done regarding the evaluation and follow-up of information security, as several of them state in the annual reports and interviews. In the search for informants, ten agencies declined to participate in the study due to a heavy workload within the information security department. One agency also responded that they could not talk about the suggested topics of the study. Thus, it may be a sensitive subject, as reports by the MSB and the National Audit Office have shown that the current situation regarding information security evaluation and follow-up is not at the desired level. The result shows that there are challenges in performing evaluation and follow-up, where key tasks such as information classification and the evaluation of security measures are described as particularly challenging. As the requirements are also unclear and there are no legitimate indicators of when activities have been fulfilled, it is difficult for government agencies to assess when they have achieved the tasks. For this reason, the study is not motivated by displaying deficiencies in the agencies' work, but rather to highlight the problems to encourage further research in this area. Hence, the result can be of interest to the governance part, but also to the agencies since the study emphasises where improvements are needed.

Recalling the objective in the Government Communication (2017/18:47) that Sweden should be the best country in the world in utilising the possibilities of digitalisation and that the public sector has a great responsibility in providing services to achieve this goal. Possibly, resources that should be used for improving information security are instead allocated to digitalisation efforts. To be the best in the world utilising digitalisation, one can argue that it is a rather challenging objective to measure. Potentially, it could be burdensome to assess when it is achieved. Similarly, the government's information security requirements are unclear, making it difficult for agencies to assess when they have been fulfilled. For example, one appropriation direction states that developing the agency should be performed with changed working methods and digitalisation, which should enable automation. Special attention should also be paid to information security. However, the appropriation direction does not describe how to work with digitalisation and which working methods to use. As a result, paying particular attention to information security becomes a challenge for the agencies, as they have no support on how to implement the changes and there are no measures to assess whether the work has been achieved. Automation is supposed to make work and processes more efficient and release resources. But with unclear instructions, the equation is difficult to solve.

Another aspect of the digitalisation topic also reflected in the results, is the fact that agencies describe the progress of digitalisation as both rapid and slow. Digitalisation is happening fast, which is forcing agencies to move at a rapid pace. As mentioned above, resources needed for information security are perhaps allocated to digitalisation projects. Also mentioned in several annual reports, many new digitalisation-related projects are announced and conducted, likely putting lots of pressure on agencies. They need to carry out their core activities, but at the same time protect their assets with a functioning information security work. Coupled with the constant stream of new digitalisation projects from the government it is reasonable to assume that there is a risk of frustration and a sense of inadequacy within agencies. If such a feeling or environment is established, there is a risk that the motivation to complete tasks including information security

evaluation and follow-up will be neglected. It is due to employees knowing there is limited time to accomplish the tasks. This phenomenon is an apparent challenge and a concern if the problem situation continues. Then it will become increasingly difficult to recruit the right skills. As one informant mentioned in the result, it is particularly important for people working with information security daily to see that their work makes a difference. If there is no time or resources to achieve such tasks, motivation could decrease. Also mentioned above, it could become a challenge to recruit employees to information security positions within government agencies if the situation persists.

Furthermore, the result indicates that all government agencies are aware of the situation, requiring improvement work. It is likely discouraging to know what to do, but not receive the right tools for conducting the work. As mentioned by Stenérus Dover, Bengtsson, and Olsson (2020), government agencies desire suggestions for what to improve, and how to follow up the improvement work. Consequently, the government should take action and provide those conditions to the agencies. One informant mentioned anticipation for the National Centre for Cybersecurity and what it can provide. However, recalling the history of the centre, and recently FRA taking over its development (DN 2023), there could be a risk that the expectation from the government agencies is too high. Despite the adjustment, there is a possibility that the centre will not possess the capability to provide the required support regarding information security. Once more, initiatives are being made, but with the fragmented governance, the efforts are insufficient to change the situation. With the government not having the right competence to govern the agencies in their information security work, the situation is difficult for the agencies since they perform their work under the provided conditions.

A further note to add to the governance topic, and previously mentioned (see subchapter 5.1), is that the agencies operate on the principle of responsibility. Consequently, the government agencies are independent but controlled by the government, thus not autonomous (Regeringen 2023a; SFS 1974:152). This fact makes it possible for government agencies to complete tasks and projects in a way that suits the particular organisation. However, since the governance and control regarding information security are weak, it is a burden for the agencies to choose the right direction. Concurrently, reports displaying the challenging situation about information security within the agencies have made the government realise that they can address the fact that the agencies are independent and should complete the majority of their work without direct involvement from the government. In that way, the government's responsibility regarding information security can be projected as less significant, making it easier to accuse the agencies of conducting inadequate work. Simultaneously, one can assume that the government itself is struggling. As mentioned in the result, information security and cybersecurity are not entirely comprehended by the civil servants at Government Offices. Hence, the work of formulating regulations and similar is not easy since they do not possess accurate information security competence. In conclusion, it all comes down to the fragmented information security governance. Without a dedicated ministry or government agency overseeing these issues, it is challenging even for the government to have control over the area. The unified approach to information security stated in the Swedish National Strategy should therefore be implemented if the situation is to improve.

5.3 Societal Aspects

The result suggests that the agencies lack resources and that it is challenging to recruit the right competence, when currently the demand for such competence is high. Consequently, agencies have been forced to postpone information security projects and one supervisory authority was not able to carry out supervision of other agencies. Concurrently, as mentioned in the introduction (see Chapter 1), agencies have been affected when information security work has not functioned accordingly. For example, the incident at the Swedish Transport Administration and cyber attacks targeting the Swedish public sector. Such incidents and attacks not only affect the work of the agencies but also citizens and society as a whole, as the agencies manage sensitive information. For example, in the case of the Swedish Transport Administration, sensitive information was disclosed that affected Sweden's national security. Despite evaluation and follow-up being internal activities performed by the agencies, they must function properly since they are part of the systematic information security work. Because if no systematic work is established, incidents occurring will likely impact actors in a relationship with the government agency.

Moreover, the result implies that the NIS2 directive and other regulations with sanctions are necessary. Since the GDPR, organisations, and agencies have become aware that they must comply with the requirements, otherwise, sanctions are imposed. Although several informants are positive about NIS2 and that it will hopefully improve information security, as well as its evaluation and follow-up. There are also some concerns that the directive will take too long to establish and that it will require work for agencies to determine whether they are affected by it. A potential risk is therefore that the assessment of the NIS2 directive could divert resources from everyday information security work. On the other hand, EU directives also have the potential to create consistent resilience to cyber threats, as member states will have to work by them, the result tells. Therefore, although such directives could take up resources, they can be positive since they bring governance and control, which is currently desired by Swedish government agencies.

As mentioned above, GDPR made government agencies and organisations aware that they must comply with requirements. Similarly, agencies will become aware that they must comply with the NIS2 directive when it has been established. However, recalling that government agencies have had difficulties complying with provisions from MSB since 2009, potentially the NIS2 implementation will be a challenge as well. As mentioned above, not only determining whether the agencies will be affected by the directive is difficult. Yet another fact is to be considered. Since MSB provisions have not been complied with, the foundation that is a systematic information security work that all agencies should work according to has not been implemented. As the result tells, the work has only recently started. Therefore, yet another regulation to comply with, which also includes sanctions will be challenging to meet. Heaps of effort will be required by government agencies, adding to the already existing pile of work. Though all agency informants are positive about the NIS2 directive, they might face a challenge demanding more work than first thought. As mentioned by one informant, the implementation of the NIS2 directive is taking too long because the efforts are needed now. Nonetheless, with the foundation not laid by the government agencies, and implicitly by the government, the time before the implementation is

perhaps convenient. Then the agencies will have the time to create a foundation consisting of systematic information security work with measures at a basic level, making them somewhat ready for the NIS2 directive.

In the result, one informant discusses that a routine procedure is to follow up on economics within organisations and government agencies. However, the information security area is still immature within organisations compared to the finical area. The result also shows that information security often is projected negatively, meaning that it is a necessity and solely a cost. Often information security is put under the IT budget, and it is a positive thing for the IT manager to keep the budget. Thus, no additional expenditures are given to information security. Additionally, since government agencies receive their funding from the government, it is important to stay within the budgetary limits each year. By shifting the focus, one can assume that tightening the alignment between the strategic objectives of a government agency and the information security objectives could improve the work. This fact is also mentioned by an informant. Currently, there is a gap between strategic objectives and security. Though, highlighting the positive impact of systematic information security work could increase the potential of making information security an attractive area to invest in. There is also a possibility that the public and private sectors could learn from each other when aligning information security and strategic objectives.

5.4 Limitations and Future Work

Ten interviews were conducted for this study, with seven informants employed by government agencies for civil preparedness. The results showed that evaluation and follow-up are performed but with varying results. The agencies have different procedures for evaluating their information security work, with some having functioning procedures. However, others express that there is no follow-up on information security, although there is an obvious desire to do so. Compiling the results of the public documents and interviews, it is clear that there is a need for clearer requirements and governance, as agencies need to prioritise which are the most important. As the content analysis of the public documents also supported the overall result, seven agency informants were considered appropriate for the study, given the time constraints. However, a possible project for future research could be to extend this study by conducting a survey of all 340 government agencies in Sweden. In this way, it would be possible to investigate whether the challenges observed concerning information security evaluation and follow-up are unique to civil preparedness agencies, or whether this is a widespread problem in all agencies. Potential findings could also emerge, providing a more comprehensive view of the problems with evaluation and follow-up. Specifically evaluation and follow-up of information security within government agencies, both in Sweden and abroad, has not been extensively researched, and the area deserves further attention.

Similarly, the choice of including the appropriation directions for the years 2021 and 2022 could be considered a limitation. However, as the content analysis ended up with analysing 152 documents, the amount of material is considered relevant for the scope of this study. Besides, only in the last couple of years, instructions regarding information security have been issued by the government. Hence, including appropriation directions from years earlier than 2021 could

have resulted in limited data to collect. Nonetheless, a suggestion for future research could be to investigate all available appropriation directions for all government agencies to produce a statistical timeline of how information security instructions have developed.

Furthermore, as the research background depicts (see subchapter 2.2.6), Sweden is not alone in having problems with information security, especially with evaluation and follow-up. Yet the research also showed that some countries are successful in their work. Therefore, future research could take on the task of comparing evaluation and follow-up procedures within government agencies in different countries to reveal success factors. The result could be used in the public sector to improve work. Some form of cooperation between countries could also be established if the project were realised.

Several challenges have been identified in the result, although this study does not provide solutions to these challenges. Therefore, future research could use this study as a basis for presenting such solutions. A possible research objective could be to develop metrics similar to KPIs but adapted for government agencies and the public sector. Such a metric could aid agencies in their evaluation and follow-up work, as it would provide clarity on requirements and objectives, and how to assess when they have been achieved.

Finally, this study included the perspective of the agencies and people involved in information security work. However, the governance perspective was not included. As the research question aimed to answer how information security is evaluated and followed up within agencies, the governance perspective was not considered necessary to answer the research question. Therefore, future research could adopt the governance perspective to learn about potential challenges in formulating regulations and providing structured governance.

6. Conclusion

The contribution of this study was to investigate how information security is evaluated and followed up within Swedish government agencies for civil preparedness. The conclusions presented are based on the qualitative content analysis of public documents, i.e. appropriation directions and annual reports for 2021 and 2022, and the results derived from the semi-structured interviews. Triangulation, that is the combination of data collection techniques, is intended to increase the validity of the research and provide greater support for the evaluation of the results (Yin 2013). The triangulation techniques are considered to have fulfilled the intentions of the study by providing what is considered to be a consistent result, supported by previous research.

To answer the research question of how information security is evaluated and followed up within the Swedish government agencies for civil preparedness, the content analysis and semi-structured interviews show that evaluation and follow-up are performed in nearly all agencies. However, the procedures are carried out differently depending on the agency. Diverse methods, models, and tools are used depending on what suits the agency. Due to unclear instructions in the appropriation directions and provisions, the methods for evaluation and follow-up appear different or non-existent. In addition, many of the investigated agencies have only recently started to work systematically with information security, so routines and working methods are yet to be established. Not long ago, information security had a low priority, but due to rapid changes in the threat landscape, it is beginning to receive increased attention. Nonetheless, implementing a systematic approach to information security is challenging because it is perceived as costly and not delivering value to the organisation. Therefore, the positive impact that information security can have on an organisation could benefit from being more widely promoted.

One should not forget that almost all agencies claim to be aware of the demanding situation and that much work is required in the near future. The awareness is positive, as being oblivious about the situation would have made things ever so challenging. However, as the study also depicted, there are issues related to a lack of resources and competence, as information security cannot be allowed to take too much focus away from the day-to-day work within agencies. In addition, depending on the area in which an agency operates, it is affected by different requirements, regulations, and rules from other regulators. This plethora of requirements makes it difficult to navigate and prioritise information security work as there are only a finite number of resources. In addition, the results suggested that the Government Office is not issuing coherent instructions on how to perform evaluation and follow-up. Therefore, the agencies are struggling since the unified approach stated in the National Strategy for Information Security and Cybersecurity (Skr. 2016/17:213) is missing.

With these agencies having responsibility for the civil preparedness of society, they also have a role in protecting Sweden. Insecurities arise with cyber attacks and a society where war is present. Hence, government agencies must be given the opportunity to protect their assets, where sensitive information of citizens is considerably included. Hence, in the public sector, the purpose of information security is not only about protecting the information of an agency. But with the

appointed responsibility toward citizens that the agencies have, they must also protect information with a high privacy value. Achieving this goal requires a systematic approach to information security across all components, from information classification to evaluation and follow-up. Accordingly, this study aimed at highlighting the important area, and argues that it has done so by providing insight into how evaluation and follow-up of information security are performed within the Swedish government agencies for civil preparedness.

References

AlGhamdi, S., Win, K.T. and Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. *Computers & Security*, 99, p. 102030. Available at: https://doi.org/10.1016/j.cose.2020.102030.

Bergquist, J.-H., Tinet, S. and Gao, S. (2021). An information classification model for public sector organizations in Sweden: a case study of a Swedish municipality. *Information & Computer Security*, 30(2), pp. 153–172. Available at: https://doi.org/10.1108/ICS-03-2021-0032.

Bergström, E., Anteryd, F. and Åhlfeldt, R.-M. (2018). Information Classification Policies: An Exploratory Investigation. In Dhillon, G. and Samonas, S. (eds) *Proceedings of the Annual Information Institute Conference*. Las Vegas, NV, 26-28 March 2018, pp. 26-28.

Bell, J. (2016). *Introduktion till forskningsmetodik*. 5th ed., Lund: Studentlitteratur.

Berndt, A.E. (2020). Sampling Methods. *Journal of Human Lactation*, 36(2), pp. 224–226. Available at: https://doi.org/10.1177/0890334420906850.

Berndtsson, M., Hansson, J., Olsson, B. and Lundell, B. (2008). *Thesis Projects A Guide for Students in Computer Science and Information Systems*. London: Springer-Verlag.

Bigdeli, A.Z., Kamal, M.M. and de Cesare, S. (2013). Electronic information sharing in local government authorities: Factors influencing the decision-making process. *International Journal of Information Management*, 33(5), pp. 816–830. Available at: https://doi.org/10.1016/j.ijinfomgt.2013.05.008.

Boehmer, W. (2008). Appraisal of the Effectiveness and Efficiency of an Information Security Management System Based on ISO 27001. In. *Second International Conference on Emerging Security Information, Systems and Technologies, 2008.*, pp. 224–231. Available at: https://doi.org/10.1109/SECURWARE.2008.7.

Boyes, H. (2015). Cybersecurity and Cyber-Resilient Supply Chains. *Technology Innovation Management Review*, 5(4), pp. 28–34.

Broderick, J.S. (2006). ISMS, security standards and security regulations. *Information Security Technical Report*, 11(1), pp. 26–31. Available at: https://doi.org/10.1016/j.istr.2005.12.001.

Busetto, L., Wick, W. and Gumbinger, C. (2020). How to use and assess qualitative research methods. *Neurological Research and Practice*, 2(1), p. 14. Available at: https://doi.org/10.1186/s42466-020-00059-z.

Culot, G. Nassimbeni, G., Podrecca, M. and Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *The TQM Journal*, 33(7), pp. 76–105. Available at: https://doi.org/10.1108/TQM-09-2020-0202.

Crowe, S., Cresswell, K., Robertson, A., Huby, G., Avery, A. and Sheikh, A. (2011). The case study approach. *BMC Medical Research Methodology*, 11(1), p. 100. Available at: https://doi.org/10.1186/1471-2288-11-100.

Dagens Nyheter DN. (2023). *DN Debatt. ”FRA får ta över ansvaret för Sveriges cybersäkerhet”*. https://www.dn.se/debatt/fra-far-ta-over-ansvaret-for-sveriges-cybersakerhet/ [Accessed: 2023-05-07]

Ekonomistyrningsverket. (n.d.). *Regleringsbrev – Statsliggaren*. https://www.esv.se/statsliggaren/ [Accessed: 2023-03-29]

Ekonomistyrningsverket. (2023). *Årsbokslut och årsredovisning*. https://www.esv.se/rapportering/ekonomiskt-utfall/arsbokslut-och-arsredovisning/ [Accessed: 2023-04-29]

Eloff, M.M. and von Solms, S.H. (2000). Information Security Management: An Approach to Combine Process Certification And Product Evaluation. *Computers & Security*, 19(8), pp. 698–709. Available at: https://doi.org/10.1016/S0167-4048(00)08019-6.

Eloff, M.M. and Eloff, J.H.P. (2003). Information Security Management System: Processes and Products. In Gritzalis, D., de Capitani di Vimercati, S., Samarati, P. and Katsikas, S. (eds) *Security and Privacy in the Age of Uncertainty*. Boston, MA: Springer US (IFIP — The International Federation for Information Processing), pp. 193–204. Available at: https://doi.org/10.1007/978-0-387-35691-4_17.

Enisa. (n.d.). *Supporting the implementation of Union policy and law regarding cybersecurity*. https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new [Accessed: 2023-03-14]

Eugen, P. and Petruţ, D. (2019). Exploring the New Era of Cybersecurity Governance. *Analele Universitatii Ovidius Constanta*, XVIII, pp. 358–363.

European Commission. (2023). *The Digital Economy and Society Index (DESI)*. https://digital-strategy.ec.europa.eu/en/policies/desi [Accessed: 2023-02-22]

Folkhälsomyndigheten. (2022). *Om lagar, förordningar och föreskrifter*. https://www.folkhalsomyndigheten.se/publikationer-och-material/foreskrifter-och-allmanna-rad/om-lagar-forordningar-och-foreskrifter/ [Accessed: 2023-03-07]

Fortifikationsverket. (n.d.). *Styrning*. https://www.fortifikationsverket.se/om-oss/styrning/ [Accessed: 2023-03-06]

Försvarsmakten. (2022). *Cyberangrepp största hotet just nu*. https://www.forsvarsmakten.se/sv/aktuellt/2022/03/cyberangrepp-storsta-hotet-just-nu/ [Accessed: 2023-03-01]

Ganji, D., Kalloniatis, C., Mouratidis, H. and Malekshahi Gheytassi, S. (2019). Approaches to Develop and Implement ISO/IEC 27001 Standard - Information Security Management Systems: A Systematic Literature Review. *International Journal on Advances in Software*, 12(3 & 4), pp. 228–238.

Ghahramani, F., Yazdanmehr, A., Chen, D. and Wang, J. (2022). Continuous improvement of information security management: an organisational learning perspective. *European Journal of Information Systems*, pp. 1–22. Available at: https://doi.org/10.1080/0960085X.2022.2096491.

Hatcher, W., Meares, W.L. and Heslen, J. (2020). The cybersecurity of municipalities in the United States: an exploratory survey of policies and practices.

Journal of Cyber Policy, 5(2), pp. 302–325. Available at: https://doi.org/10.1080/23738871.2020.1792956.

Hedström, K., Kolkowska, E., Karlsson, F. and Allen, J.P. (2011). Value conflicts for information security management. *The Journal of Strategic Information Systems*, 20(4), pp. 373–384. Available at: https://doi.org/10.1016/j.jsis.2011.06.001.

Horne, C., Ahmad, A. and Maynard, S. (2016). A Theory on Information Security. In *The 27th Australasian Conference on Information Systems*. Wollongong, Australia.

Horne, C. (2018). *Understanding Information Security Strategy in Organisations*. Doctor of Philosophy, Department of Computing and Information Systems. The University of Melbourne. https://www.researchgate.net/publication/339710294 Understanding Information Security Strategy in Organisations

Informationssäkerhet.se. (2015). *Samverkansgruppen för informationssäkerhet*. https://www.informationssakerhet.se/om-informationssakerhet2/samverkansgruppen-for-informationssakerhet/ [Accessed: 2023-03-06]

Informationssäkerhet.se. (2020a). *Metodstödet*. https://www.informationssakerhet.se/metodstodet/metodstodet/ [Accessed: 2023-02-28]

Informationssäkerhet.se. (2020b). *Följa upp och förbättra*. https://www.informationssakerhet.se/metodstodet/folja-upp-och-forbattra/ [Accessed: 2023-02-28]

Informationssäkerhet.se. (2020c). *Rättsliga krav på informationssäkerhet i olika verksamheter*. https://www.informationssakerhet.se/lagar--regelverk/rattsliga-krav-pa-informationssakerhet-i-olika-verksamheter/ [Accessed: 2023-03-07]

Informationssäkerhet.se. (2021). *Förordningar och föreskrifter*. https://www.informationssakerhet.se/lagar--regelverk/forordningar-och-foreskrifter/ [Accessed: 2023-03-07]

Informationssäkerhetsutredningen. (2015). *Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten (SOU 2015:23)*. Stockholm: Justitiedepartementet. https://www.regeringen.se/contentassets/8ae8ef6d5d3f45058c981cbab4e297de/informations--och-cybersakerhet-i-sverige.-strategi-och-atgarder-for-saker-information-i-staten-sou-201523

International Standardization Organization ISO. (2018). *ISO/IEC 27000:2018(en) Information technology — Security techniques — Information security management systems — Overview and vocabulary*. https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en [Accessed: 2023-02-22]

ITU. (2023). *Global Cybersecurity Index 2020*. https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E [Accessed: 2023-02-22]

Izurieta, R.R., Jhony Caucha Morales, L., Toapanta Toapanta, S.M., Gallegos, L.E.M. and Orizaga Trejo, J.A. (2021). Analysis of the Information Security of

Public Organizations in Ecuador. In *2021 International Conference on Computational Science and Computational Intelligence (CSCI)*. Las Vegas, NV, pp. 823–829. Available at: https://doi.org/10.1109/CSCI54926.2021.00195.

Jonathan, G.M. (2020). Digital Transformation in the Public Sector: Identifying Critical Success Factors. In Themistocleous, M. and Papadaki, M. (eds) *Information Systems. Information Systems. EMCIS 2019. Lecture Notes in Business Information Processing, vol 381*, Cham: Springer International Publishing, pp. 223–235. Available at: https://doi.org/10.1007/978-3-030-44322-1_17.

Jonathan, G.M., Hailermariam, K.S., Gebremeskel, B.K. and Yalew, S.D. (2021). Public Sector Digital Transformation: Challenges for Information Technology Leaders. In *2021 IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*. Vancouver, BC, pp. 1027–1033. Available at: https://doi.org/10.1109/IEMCON53756.2021.9623161.

Karlsson, F., Hedström, K., Prenkert, F., Kolkowska, E. and Helin, S. (2021). Attempts to share information between public sector organisations over time: A case-based exploration of value conflicts. *Information Polity*, 26(3), pp. 289–310. Available at: https://doi.org/10.3233/IP-200234.

Karlsson, F., Hedström, K. and Goldkuhl, G. (2017). Practice-based discourse analysis of information security policies. *Computers & Security*, 67, pp. 267–279. Available at: https://doi.org/10.1016/j.cose.2016.12.012.

Khando, K., Gao, S., Islam S.M. and Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security*, 106, p. 102267. Available at: https://doi.org/10.1016/j.cose.2021.102267.

Leedy, P.D. & Ormrod, J.E. (2015). *Practical Research Planning and Design*. 11th ed., Harlow: Pearson Education Limited.

Lenning, J. and Gremyr, I. (2021). Unleashing the potential of internal audits: a review and research agenda. *Total Quality Management & Business Excellence*, 33(13), pp. 1–17. Available at: https://doi.org/10.1080/14783363.2021.1911635.

Loukis, E. and Spinellis, D. (2001). Information Systems Security in the Greek Public Sector. *Information Management & Computer Security*, 9. Available at: https://doi.org/10.1108/09685220110366740.

Masilela, L. and Nel, D. (2021). The role of data and information security governance in protecting public sector data and information assets in national government in South Africa. *Africa's Public Service Delivery and Performance Review*, 9(1), pp. 1–10. Available at: https://doi.org/10.4102/apsdpr.v9i1.385.

Meyerhoff Nielsen, M. (2019). Governance lessons from Denmark's digital transformation. In *Proceedings of the 20th Annual International Conference on Digital Government Research*. Dubai, United Arab Emirates: ACM, pp. 456–461. Available at: https://doi.org/10.1145/3325112.3329881.

MSBFS 2020:6. *Föreskrifter om informationssäkerhet för statliga myndigheter*. Myndigheten för samhällsskydd och beredskap.

MSBFS 2020:7. *Föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter*. Myndigheten för samhällsskydd och beredskap.

Myers, M.D. and Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and Organization*, 17(1), pp. 2–26. Available at: https://doi.org/10.1016/j.infoandorg.2006.11.001.

Myndigheten för Digital Förvaltning DIGG. (2023). *Digitala Sverige 2022 En samlad analys av samhällets digitalisering*. https://www.digg.se/download/18.1e68c05518649f2b2eb6a8e/1677659508496/Digitala%20Sverige%202022.pdf

Myndigheten för samhällsskydd och beredskap MSB. (2015). *Informationssäkerheten i Sveriges kommuner Analys och rekommendationer utifrån MSB:s kommunenkät 2015*. https://rib.msb.se/filer/pdf/28222.pdf

Myndigheten för samhällsskydd och beredskap MSB. (2021a). *Kompetens inom informations och cybersäkerhet En förstudie om kompetensförsörjning för samhället*. https://www.informationssakerhet.se/siteassets/kompetensutveckling/kompetens-inom-informations--och-cybersakerhet---en-forstudie-om-kompetensforsorjning-for-samhallet.pdf

Myndigheten för samhällsskydd och beredskap MSB. (2021b). *Nationellt center för cybersäkerhet*. https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/nationellt-center-for-cybersakerhet/ [Accessed: 2023-03-06]

Myndigheten för samhällsskydd och beredskap MSB. (2022a). *Det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen - Resultatredovisning Infosäkkollen 2021*. https://rib.msb.se/filer/pdf/30002.pdf [Accessed: 2023-02-28]

Myndigheten för samhällsskydd och beredskap MSB. (2022b). *Om systematiskt informationssäkerhetsarbete.* https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/systematiskt-informationssakerhetsarbete/om-systematiskt-informationssakerhetsarbete/ [Accessed: 2023-03-03]

Myndigheten för samhällsskydd och beredskap MSB. (2022c). *Samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022 – redovisning 2022*. https://www.fmv.se/globalassets/dokument/verksamhet/2022-ars-samland-informations-och-cybersakerhetshandlingsplan-2019-2022.pdf

Myndigheten för samhällsskydd och beredskap MSB. (2022d). *NIS-direktivet*. https://www.msb.se/nis [Accessed: 2023-03-07]

Myndigheten för samhällsskydd och beredskap MSB. (2022e). *Nytt beredskapssystem träder i kraft den 1 oktober*. https://www.msb.se/sv/aktuellt/nyheter/2022/september/nytt-beredskapssystem-trader-i-kraft-den-1-oktober/ [Accessed: 2023-05-09]

Myndigheten för samhällsskydd och beredskap MSB. (2023a). *Strukturreform av krisberedskap och civilt försvar*. https://www.msb.se/sv/amnesomraden/krisberedskap--civilt-forsvar/det-svenska-civila-beredskapssystemet/strukturreform-av-krisberedskap-och-civilt-forsvar/ [Accessed: 2023-03-03]

Myndigheten för samhällsskydd och beredskap MSB. (2023b). *När kriget kom nära – Årsrapport it-incidentrapportering 2022*. https://rib.msb.se/Filer/pdf/30339.pdf

Norris, D.F., Mateczun, L., Joshi, A. and Finin, T. (2019). Cyberattacks at the Grass Roots: American Local Governments and the Need for High Levels of Cybersecurity. *Public Administration Review*, 79(6), pp. 895–904. Available at: https://doi.org/10.1111/puar.13028.

Paananen, H., Lapke, M. and Siponen, M. (2020). State of the art in information security policy development. *Computers & Security*, 88, p. 101608. Available at: https://doi.org/10.1016/j.cose.2019.101608.

Park, C.-S., Jang, S.-S. and Park, Y.-T. (2010). A study of Effect of Information Security Management System [ISMS] Certification on Organization Performance. *International Journal of Computer Science and Network Security*, 10(3), pp. 10–21. Available at: https://doi.org/10.5762/KAIS.2012.13.9.4224.

Patel, R. & Davidson, B. (2019). *Forskningsmetodikens grunder*. 5th ed., Lund: Studentlitteratur.

Plesner, U., Justesen, L. and Glerup, C. (2018). The transformation of work in digitized public sector organizations. *Journal of Organizational Change Management*, 31(5), pp. 1176–1190. Available at: https://doi.org/10.1108/JOCM-06-2017-0257.

Posthumus, S. and von Solms, R. (2004). A framework for the governance of information security. *Computers & Security*, 23(8), pp. 638–646. Available at: https://doi.org/10.1016/j.cose.2004.10.006.

Post- och telestyrelsen. (2022). *Regleringsbrev och instruktion*. https://www.pts.se/sv/om-pts/verksamhet/regleringsbrev-och-instruktion/ [Accessed: 2023-03-06]

Regeringen. (2023a). *Myndigheter och bolag med statligt ägande*. https://www.regeringen.se/sa-styrs-sverige/myndigheter-och-bolag-med-statligt-agande/ [Accessed: 2023-03-06]

Regeringen. (2023b). *Nationell strategi för samhällets informations- och cybersäkerhet*. https://www.regeringen.se/regeringens-politik/krisberedskap/nationell-strategi-for-samhallets-informations--och-cybersakerhet/ [Accessed: 2023-03-06]

Regeringens skrivelse 2016/17:213. (2017). *Nationell strategi för samhällets informationsoch cybersäkerhet*. https://www.regeringen.se/contentassets/3f89e3c77ad74163909c092b1beae15e/nationell-strategi-for-samhallets-informations--och-cybersakerhet-skr.-201617213 [Accessed: 2023-03-03]

Regeringens skrivelse 2017/18:47. *Hur Sverige blir bäst i världen på att använda digitaliseringens möjligheter – en skrivelse om politikens inriktning*. https://www.regeringen.se/rattsliga-dokument/skrivelse/2017/11/skr.-20171847 [Accessed: 2023-02-22]

Reid, R. and Van Niekerk, J. (2014). From information security to cyber security cultures. In *2014 Information Security for South Africa. 2014 Information Security for South Africa*, pp. 1–7. Available at: https://doi.org/10.1109/ISSA.2014.6950492.

Riksdagsförvaltningen. (2020). *Riksdagens flerspråkiga ordlista*. https://www.riksdagen.se/globalassets/15.-bestall-och-ladda-ned/informationsmaterial/riksdagens-flersprakiga-ordlista-nov-2020.pdf

Riksrevisionen. (2016). *Informationssäkerhetsarbete på nio myndigheter (RiR 2016:8)*. Stockholm: Riksrevisionen. https://www.riksrevisionen.se/download/18.78ae827d1605526e94b2dbec/1518435509192/RiR_2016_8_INFOSAK2_WEBB.pdf

Riksrevisionen. (2023). *Regeringens styrning av samhällets informations- och cybersäkerhet – både brådskande och viktig*. https://www.riksrevisionen.se/download/18.4aeb2da8187b22973fb2828/1682339418438/RiR_2023_8_rapport.pdf

Royal Swedish Academy of Engineering Sciences IVA. (2022). *Cybersäkerhet för ökad konkurrenskraft*. https://www.iva.se/globalassets/bilder/projekt/cybersakerhet/202210-iva-cybersakerhet-rapport.pdf

Saunders, M., Lewis, P. & Thornhill, A. (2007). *Research Methods for Business Students*. 4th ed., Harlow: Pearson Education Limited.

Schultze, U. and Avital, M. (2011). Designing interviews to generate rich data for information systems research. *Information and Organization*, 21(1), pp. 1–16. Available at: https://doi.org/10.1016/j.infoandorg.2010.11.001.

SecurityUser.com. (2023). *"Ryska Killnet bakom cyberattacker mot svenska myndigheter"*. https://www.securityuser.com/se/Nyheter/Samhalle/ryska-killnet-bakom-cyberattacker-mot-svenska-myndigheter [Accessed: 2023-03-01]

SFS 1974:152. *Regeringsformen*. Justitiedepartementet.

SFS 2007:515. *Myndighetsförordning*. Finansdepartementet.

SFS 2016:658. *Säkerhetsskyddsförordning*. Justitiedepartementet.

SFS 2018:585. S*äkerhetsskyddslag*. Justitiedepartementet.

SFS 2018:1174. *Lag om informationssäkerhet för samhällsviktiga och digitala tjänster*. Försvarsdepartementet.

SFS 2018:1175. *Förordning om informationssäkerhet för samhällsviktiga och digitala tjänster*. Försvarsdepartementet.

SFS 2022:524. *Förordning om statliga myndigheters beredskap*. Försvarsdepartementet.

Siponen, M.T. and Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, 38(1), pp. 60–80. Available at: https://doi.org/10.1145/1216218.1216224.

Siponen, M. and Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management*, 46(5), pp. 267–270. Available at: https://doi.org/10.1016/j.im.2008.12.007.

Stafford, T., Deitz, G. and Li, Y. (2018). The role of internal audit and user training in information security policy compliance. *Managerial Auditing Journal*, 33(4), pp. 410–424. Available at: https://doi.org/10.1108/MAJ-07-2017-1596.

Stahl, B.C., Doherty, N.F. and Shaw, M. (2012). Information security policies in the UK healthcare sector: a critical evaluation. *Information Systems Journal*, 22(1), pp. 77–94. Available at: https://doi.org/10.1111/j.1365-2575.2011.00378.x.

Statskontoret. (2023). *Myndigheterna under regeringen*. https://www.statskontoret.se/fokusomraden/fakta-om-statsforvaltningen/fakta-om-statsforvaltningen/ [Accessed: 2023-04-29]

Steinbart, P.J., Raschke, R.L., Gal, G. and Dilla, W.N. (2012). The relationship between internal audit and information security: An exploratory investigation. *International Journal of Accounting Information Systems*, 13(3), pp. 228–243. Available at: https://doi.org/10.1016/j.accinf.2012.06.007.

Stenerus, A.-S., Bengtsson, J. and Olsson, M. (2020). *IT-incidenter på statliga myndigheter. Orsaker till utebliven rapportering*. FOI-R--4815--SE. Available at: https://www.foi.se/rest-api/report/FOI-R--4815--SE.

Sveriges riksdag. (2022). *Grundlagarna*. https://www.riksdagen.se/sv/sa-funkar-riksdagen/demokrati/grundlagarna/ [Accessed: 2023-03-06]

SVT Nyheter. (2019). *Transportstyrelsen – detta har hänt*. https://www.svt.se/nyheter/inrikes/transportstyrelsen-detta-har-hant [Accesssed: 2023-02-24]

Szczepaniuk, E.K., Szczepaniuk, H., Rokicki, T. and Klepacki, B. (2020). Information security assessment in public administration. *Computers & Security*, 90, p. 101709. Available at: https://doi.org/10.1016/j.cose.2019.101709.

SÄPO. (2023a). *Säkerhetspolisen 2022–2023*. https://www.sakerhetspolisen.se/download/18.36cda2851868025da5b2b/1677241538918/SP_A%CC%8Arsbok_2022__Anpassad.pdf

SÄPO. (2023b). *Styrning och uppföljning*. https://sakerhetspolisen.se/om-sakerhetspolisen/styrning-och-uppfoljning.html [Accessed: 2023-04-29]

Thompson, N., Mullins, A. and Chongsutakawewong, T. (2020). Does high e-government adoption assure stronger security? Results from a cross-country analysis of Australia and Thailand. *Government Information Quarterly*, 37(1), p. 101408. Available at: https://doi.org/10.1016/j.giq.2019.101408.

Transportstyrelsen. (2023). *Frågor och svar kring uppgifter i media om vår itupphandling*. https://www.transportstyrelsen.se/sv/Om-transportstyrelsen/fragor-och-svar/ [Accessed: 2023-02-24]

Tu, Z. and Yuan, Y. (2014). Critical Success Factors Analysis on Effective Information Security Management: A Literature Review. *Information Systems Security* [Preprint].

Turell, J., Su, F. and Boulanin, V. (2020) *Cyber-incident Management: Identifying and Dealing with the Risk of Escalation*. 55. Available at: https://sipri.org/sites/default/files/2020-11/sipripp55.pdf

Tuya, M.D. and Tuya, M.L.D. (2019). Creating Value Through Information and Knowledge Flow: Lessons from the Public Sector Applied to the Private Sector. *Journal of Creating Value*, 5(2), pp. 210–221. Available at: https://doi.org/10.1177/2394964319851951.

van Veenstra, A.F. and Ramilli, M. (2011). Exploring Information Security Issues in Public Sector Inter-organizational Collaboration. In Janssen, M., Scholl, H.J., Wimmer, M.A. and Tan, Y. (eds) *Electronic Government*. Berlin, Heidelberg: Springer (Lecture Notes in Computer Science), pp. 355–366. Available at: https://doi.org/10.1007/978-3-642-22878-0_30.

von Solms, R. and van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, pp. 97–102. Available at: https://doi.org/10.1016/j.cose.2013.04.004.

von Solms, B. and von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security*, 23(5), pp. 371–376. Available at: https://doi.org/10.1016/j.cose.2004.05.002.

Walsham, G. (2006). Doing Interpretive Research. *EJIS*, 15, pp. 320–330. Available at: https://doi.org/10.1057/palgrave.ejis.3000589.

Warkentin, M. and Orgeron, C. (2020). Using the security triad to assess blockchain technology in public sector applications. *International Journal of Information Management*, 52, p. 102090. Available at: https://doi.org/10.1016/j.ijinfomgt.2020.102090.

Williams, P. (2001). Information Security Governance. *Information Security Technical Report*, 6(3), pp. 60–70. Available at: https://doi.org/10.1016/S1363-4127(01)00309-0.

Yin, R.K. (2009). *Case Study Research Design and Methods*. 4th ed., Thousand Oaks: Sage Publication.

Yin, R.K. (2013). Validity and generalization in future case study evaluations. *Evaluation*, 19(3), pp. 321–332. Available at: https://doi.org/10.1177/1356389013497081.

Yusif, S. and Hafeez-Baig, A. (2021). A Conceptual Model for Cybersecurity Governance. *Journal of Applied Security Research*, 16, pp. 1–24. Available at: https://doi.org/10.1080/19361610.2021.1918995.

Åhlfeldt, R.-M., Nohlberg, M., Söderström, E., Lennerholt, C. and van Laere, J. (2018). Current Situation Analysis of Information Security Level in Municipalities. *Journal of Information System Security*, 14(1), pp. 3–19.

Ödlund, A. (2007). *Interorganisatorisk samverkan som nationell resurs i krishanteringen*. User report FOI-R--2425--SE. Stockholm. Available at: https://www.foi.se/rest-api/report/FOI-R--2425--SE.

Appendix A

Interview Protocol – Government agency informant

1. **Background information**
    - Can you briefly describe your professional background?
    - What is your current function or role?

2. **The government agency's role within information security**
    - Briefly describe how the information security work looks like within the government agency!
    - Specifically, how does your government agency work with information security evaluation and follow-up?

3. **Governance and control**
   This is a quotation from The Swedish National Strategy for Information Security and Cybersecurity and it states: "Regeringen skall verka för, att öka tydligheten i myndighetsstyrningen och lyfta betydelsen av ett tillfredsställande informationssäkerhetsarbete internt på myndigheterna" (Skr. 2016/17:213, 2016, p. 11)
    - What is the agency's view regarding information security governance and control from the Swedish Government/Parliament?
        - Is there anything missing?
        - Is there a need for development?
    - Are the reporting requirements in the government's appropriation directions adequate?
        - Do they provide enough knowledge about the necessary work that the agency must conduct?
        - Why/why not?
    - Except from governing appropriation directions, and the provisions from MSB – is there a need for additional policy instruments, guidelines or supporting tools?
        - Could MSB contribute with additional support?

4. **Evaluation and follow-up**
   This is a quotation from the MSB provision 2020:6 and it states: "Uppföljning av informationssäkerhetsarbetet 14 § Myndigheten ska minst en gång per år följa upp att informationssäkerhetsarbetet svarar mot myndighetsledningens målsättning och inriktning, genom att sammanställa och analysera resultatet av genomförda
   1. utvärderingar av interna regler, arbetssätt och stöd enligt 5 § p. 5,
   2. informationsklassningar enligt 6 § p. 1,
   3. riskbedömningar enligt 6 § p. 2,
   4. utvärderingar av säkerhetsåtgärder enligt 6 § p. 4, och
   5. utvärderingar av att interna regler, arbetssätt och stöd används på avsett sätt enligt 9 § p. 3." (MSBFS 2020:6, 2020, p. 6)

- Going through the above points (1–5), whichever point(s) is the most challenging to implement, and/or achieve?
    - Why?

It is stated in the general advice in 14 § in MSBFS 2020:6 that: ”Uppföljningen av myndighetens informationssäkerhetsarbete bör hållas samman av den eller de som utsetts att leda och samordna informationssäkerhetsarbetet vid myndigheten.”

- Does the agency have such appointed leaders, or does someone else conduct the follow-up?

Nowadays, some government agencies do have dedicated security officers in the top management.

- Is that true for your government agency?
- If yes, has that changed the work with information security evaluation and follow-up?
    - In what way?

5. What can be done in the future

As the NIS2 directive is incorporated into Swedish law, the number of sectors will increase to include the entire public sector.

- Will the NIS2 directive affect the work of the agency regarding information security evaluation and follow-up?
    - Why/why not?
- Would an extended mandate (supervision) for MSB or some other supervisory authority to regulate and direct agencies in their information security work be of interest?
    - Would the possibility of imposing fines or similarly improve the situation?
- Disregarding the cost and any legal obstacles, what would an ISO 27001 certification requirement imply to the government agency?
    - Would it improve information security evaluation and follow-up?
- What are, according to your government agency the biggest challenges with information security evaluation and follow-up looking ahead?

6. Ending

- Is there anything you would like to add?
- Do you have any further questions?
- Would you like to receive the finished report?

Appendix B

Interview Protocol – Senior information security informant

1. **Background information**
    - Can you briefly describe your professional background?
    - What is your current function or role?
    - How do you work with information security daily?

2. **The role of MSB within information security**
    - Regarding your background, where you have worked at MSB, in what way has MSB's work with information security evaluation and follow-up changed during the years?

3. **Governance and control**
   This is a quotation from The Swedish National Strategy for Information Security and Cybersecurity and it states: "Regeringen skall verka för, att öka tydligheten i myndighetsstyrningen och lyfta betydelsen av ett tillfredsställande informationssäkerhetsarbete internt på myndigheterna" (Skr. 2016/17:213, 2016, p. 11)
    - What is the agency's view regarding information security governance and control from the Swedish Government/Parliament?
        - Is there anything missing?
        - Is there a need for development?
    - Are the reporting requirements in the government's appropriation directions adequate?
        - Do they provide enough knowledge about the necessary work that the agency must conduct?
        - Why/why not?
    - Except from governing appropriation directions, and the provisions from MSB – is there a need for additional policy instruments, guidelines or supporting tools?

4. **Evaluation and follow-up**
   This is a quotation from the MSB provision 2020:6 and it states: "Uppföljning av informationssäkerhetsarbetet 14 § Myndigheten ska minst en gång per år följa upp att informationssäkerhetsarbetet svarar mot myndighetsledningens målsättning och inriktning, genom att sammanställa och analysera resultatet av genomförda
   1. utvärderingar av interna regler, arbetssätt och stöd enligt 5 § p. 5,
   2. informationsklassningar enligt 6 § p. 1,
   3. riskbedömningar enligt 6 § p. 2,
   4. utvärderingar av säkerhetsåtgärder enligt 6 § p. 4, och
   5. utvärderingar av att interna regler, arbetssätt och stöd används på avsett sätt enligt 9 § p. 3." (MSBFS 2020:6, 2020, p. 6)
    - Going through the above points (1–5), whichever point(s) is the most challenging to implement, and/or achieve?
        - Why?

It is stated in the general advice in 14 § in MSBFS 2020:6 that: ”Uppföljningen av myndighetens informationssäkerhetsarbete bör hållas samman av den eller de som utsetts att leda och samordna informationssäkerhetsarbetet vid myndigheten.”

- Do you have any idea whether it occurs in the way that the general advice states, or are there factors that indicate that someone else conducts the follow-up?

Nowadays, some government agencies do have dedicated security officers in the top management.

- Are there factors indicating that it has that changed the work with information security evaluation and follow-up?
    - If yes, in what way?

5. What can be done in the future

As the NIS2 directive is incorporated into Swedish law, the number of sectors will increase to include the entire public sector.

- Will the NIS2 directive affect the work of government agencies regarding information security evaluation and follow-up?
    - Why/why not?
- Would an extended mandate (supervision) for MSB or some other supervisory authority to regulate and direct agencies in their information security work be of interest?
    - Would the possibility of imposing fines or similarly improve the situation?
- Disregarding the cost and any legal obstacles, what would an ISO 27001 certification requirement imply to the government agency?
    - Would it improve information security evaluation and follow-up?
    - Are you aware of any government agencies certified according to ISO 27001?
- What are the biggest challenges with information security evaluation and follow-up for government agencies looking ahead?

6. Ending

- Is there anything you would like to add?
- Do you have any further questions?
- Would you like to receive the finished report?