Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

Vilde Nylund Johnsen

Security governance: the board's responsibility

Master's thesis in Master in Information Security
Supervisor: Einar Arthur Snekkenes
June 2023

NTNU
Norwegian University of
Science and Technology

Vilde Nylund Johnsen

Security governance: the board's responsibility

Master's thesis in Master in Information Security
Supervisor: Einar Arthur Snekkenes
June 2023

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

NTNU
Norwegian University of
Science and Technology

Acknowledgements

I would like to acknowledge and provide a great thanks to my supervisor, Einar Arthur Snekkenes, for his great contribution of knowledge and valuable advice during this master thesis.

Furthermore, I would like to express warm gratitude to one of my resources and supplementary supervisors, Mari Nylund. Mari has helped conduct the interview guide as well as provided relevant resources and guidelines to conduct a well-accomplished master thesis.

I must also acknowledge my great appreciation to the participants during this master thesis and their time and resources in answering all my interview questions.

Lastly, I would like to acknowledge The Institute of Internal Auditors, Norwegian Standard, and Næringslivets Sikkerhetssråd for their consent of copyrights to relevant figures presented in this master thesis.

Abstract

The aim for this master thesis is to examine how companies work with evaluation as an element of their security governance and what potential lies in this process to ensure effective governance and control of the business' security level and compliance. This thesis is based on qualitative research and uses interviews to determine which experiences different companies and controlling authorities have and to what extent the evaluation process is used and provides value. Furthermore, the answers provided in the interviews will be used to answer the different research questions given in this master thesis.

The research revealed that very few companies are familiar with the governance processes as they are addressed in ISO 27014. Furthermore, several companies do not have the right equipment, such as tools and processes, that provide a reasonable data basis to evaluate the state of security. Mainly, it is the top management that participates in the management review. In addition, due to a lack of culture, maturity, and competence, it is difficult for companies to understand how to utilize the evaluation process. This may also be why the companies and the controlling authorities vary in correspondence.

Based on the data collection in this study, the governing body will significantly benefit from adopting ISO 27014, and the evaluation process in particular, to understand the threat picture and determine areas of governance and criteria for evaluating security performance. Furthermore, ISO 27014 will provide a great potential gain when establishing a "communication bridge" between the board and the top management. To a certain extent, this could be delivered by the evaluation process, handled by the governing body itself, or a corporate GRC function.

Sammendrag

I denne master oppgaven vil det bli undersøkt hvordan virksomheter jobber med evaluering som et element i sin sikkerhetsstyring, og hvilke potensiale som ligger i denne prosessen for å sikre effektiv styring og kontroll med virksomhetens sikkerhetsnivå og etterlevelse. Denne oppgaven baserer seg på kvalitativ metode og tar i bruk intervjuer for å få svar på spørsmål knyttet til erfaringer ulike virksomheter og kontroll myndigheter har og i hvilken grad evalueringsprosessen blir brukt og gir verdi. Videre vil svarene gitt i intervjuene bli brukt for å svare på de ulike forskningsspørsmålene gitt i denne master oppgaven.

Undersøkelsen avslører at det er svært få virksomheter som er kjent med styringsprosessene slik de er addressert i ISO 27014. Videre, flere virksomheter har ikke de riktige redskapene, som verktøy og prosesser, som gir et godt datagrunnlag for evaluering av sikkerhetstilstand. I all hovedsak er det konsernledelsen som deltar i ledelsens gjennomgang. I tillegg til dette, grunnet mangel på kultur, modenhet og kompetanse, er det vanskelig for virksomhetene å forstå hvordan de kan nyttiggjøre evalueringsprosessen. Dette kan også være en årsak til hvorfor det varierer med samsvar mellom virksomhetene og kontroll myndighetene.

Basert på datainnsamlingen i denne undersøkelsen vil det styrende organet ha betydelig nytte av å ta i bruk ISO 27014, og evalueringsprosessen spesielt, for å forstå trusselbildet og bestemme styringsområder og kriterier for evaluering av sikkerhetsytelse. Videre vil ISO 27014 gi en stor potensiell gevinst ved etablering av en «kommunikasjonsbro» mellom styret og toppledelsen. Til en viss grad kan dette leveres av evalueringsprosessen, håndtert av det styrende organet selv, eller en bedrifts GRC-funksjon.

Contents

Figures

Tables

Chapter 1

Introduction

1.1 Topic covered by the project

In light of today's threat landscape and geopolitical tensions, there is a greater need to have a greater risk perspective than before, as well as invest in control mechanisms and ensure effective governance. Information Security Governance is an essential aspect of an enterprise and is necessary to perform well security management. There are many areas of governance within an entity where each governance area is a component of the overall governance objectives of an entity and thus should be aligned with the discipline of the entity. In security governance, various management activities are carried out, which are necessary for the enterprise to prioritize and address risks efficiently. Through governance, an organization will also achieve compliance between laws and regulations. Effective governance of information security requires both members of the governing body and managers to fulfill their respective roles in a consistent way [1].

According to Internal Organization for Standardization (ISO) 27014, the definition of governance of information security is the means by which an organization's governing body provides overall direction and control of activities that affect the security of an organization's information [2]. The security governance system in this context means the resources and elements that, together across the organization, contribute to identifying, establishing, and maintaining a level of security per the goals and requirements set.

According to ISO 27001, the definition of information security management is associated with ensuring the achievement of the organization's objectives described within the strategies and policies established by the governing body [3]. In other words, information security management is more about planning and carrying out the activities needed to achieve the goals.

1.2 Keywords

Information Security Governance, Information Security Management, Governing body, Top Management, Well-functioning board, Entity, Organization.

1.3 Problem description

Digital threats represent a critical risk to both small and large companies alike. The governing body must understand digital threats and risks well and ensure that the risks are discovered and managed according to established frameworks and verified by third parties [4]. It is also a corporate responsibility that must be fully integrated into the business, such as sustainability. Furthermore, there is a knowledge and communication gap in digital security, in which boards and management lack the capacity to understand the risks. Board members should exemplify certain qualities to counter this, including inquisitiveness, patience, braveness, alertness, and open-mindedness [4].

Several research articles focusing on information security governance look at one or more important aspects of digital security [5–7]. However, these articles do not consider the value of the governance processes, particularly the evaluation process. The importance of discovering and managing corporate threats and risks is discussed in terms of established frameworks. For example, Da Veiga and Eloff mention that due to the increased threat landscape and critical risks, there is a greater need to ensure effective governance [5]. Still, the essence of governance processes, particularly the evaluation process, is not discussed.

The definition of critical infrastructure is becoming more comprehensive now that critical infrastructure goes across national borders, and data and services are moved to servers controlled by large international companies [8, 9]. Due to the rapid and unclear digitization, there is an enormous need to get a better overview, an understanding of the stakeholder's interests, and better governance in the business. If the organization is not fully equipped to understand the security condition, including the possible risks and deviation, the consequences may be catastrophic. The evaluation process is integral to getting a complete systematic overview to ensure that the basis for governance and control is better.

The problem description for this task is:

"To what extent can evaluation of security, as defined in ISO 27014, contribute to strengthening interaction between the security management, the top management, and the governing bodies?"

1.4 Justification, motivation and benefits

According to The Norwegian National Security Authority (NSM) in the report 'Security expert advice: A resilient Norway,´ there is a greater need for a more threat-based "precautionary" approach to preventing unwanted actors from gaining a foothold in Norway [8]. The authorities and businesses must be more robust and resistant to activities that could become acute threats to national security. It is difficult to see other better alternatives to prevent this than well-functioning governance systems throughout the value chain of critical functions in Norway.

Of the governance processes addressed in ISO 27014, it is examined whether the evaluation process is a key process as an examination of all the governance processes would be too extensive. Furthermore, the evaluation process is the process that is closest to the board. Through good facilitation of the evaluation process, the business will be able to better manage and monitor in the form of delimitation and avoid the loss of severe critical infrastructure in the event of a security incident [2, 8].

The cyber attack against Hydro in 2019 is a significant example where the case has not yet been concluded and has led to enormous consequences that cost the company 800 million NOK [10, 11]. This has also had significant economic implications for society. In the aftermath of the attack, ten officers from Kripos led the investigation in collaboration with 45 foreign and a hundred Ukrainian police officers. Integrating the evaluation process into the business will not necessarily prevent security incidents, but the company will be more resilient and thus reduce such social consequences.

1.5 Research questions

This master thesis examines how companies work with evaluation as an element of their security governance and what potential lies in this process to ensure effective governance and control of the business' security level and compliance. Furthermore, it will be investigated how the evaluation process can add more value, become more efficient and ensure that the basis for governance and control is better. The next step is to use the obtained information to understand how the companies operate with the evaluation process and what's included in this process.

The research questions for this master thesis is:

- *To what extent are management systems known and used?*
- *What is used to evaluate the state of security and to what extent is this a justified state?*
- *Which roles are involved in evaluating security performance?*

- *What is needed to reduce the uncertainty surrounding the state of security?*
- *Is there a correspondence between the supervisory authorities' experiences and the companies answers?*

1.6 Summary of contributions

The planned contribution for this master thesis is to map the evaluation process in terms of what is used most and is most important to have available. Furthermore, the master thesis will provide awareness among companies and the essence of the evaluation process. Lastly, it shall promote further work to take the results to the next level.

1.7 Thesis structure

Chapter 1 introduces the topic covered by the project, the problem description, justification, motivation, benefits, research questions, and a short summary of contributions. In Chapter 2, all theories highlighted in the interview questions are described and lay the foundation for the academic content of the thesis. Chapter 3 describes the various methods used during the project to conduct the interviews and analyze the results. The interview questions are described in Chapter 4 and divided into categories with associated descriptions of theories and purposes that apply in each category. The analysis itself is described in Chapter 5, where the data collected through the interviews are summarized and illustrated using figures.

The results are discussed in Chapter 6 by answering questions related to purposes described in the interview guide and reflections made through the interview process. Future work, including limitations encountered during this master thesis, is proposed and described in Chapter 7. Finally, the conclusion comes in Chapter 8, where the research questions and the problem description are answered and concluded.

Chapter 2

Related work

The theory chapter consists of several sections where each part describes in detail a theory relevant to this master's thesis. To analyze whether the data collection corresponds to existing theory, the report will be based on a large amount of theory. Definitions are clearly described to ensure a common understanding of the terms. This is important to prevent different term definitions from creating misunderstandings that can affect the result of the assignment. This also applies to legislation and which businesses are subject to which laws and regulations, and whether these laws set requirements for the evaluation process. Last is the state-of-the-art analysis, where different research articles aligned with the research questions in section 1.5 are described.

Many businesses use frameworks that specify and set requirements for the company and the evaluation process. Businesses that do not use frameworks may give different answers and do things differently, impacting the task. Articles and reports will also be relevant to the assignment due to experience and specific figures on additional data.

2.1 Definitions

Clear definitions are necessary to understand this master's thesis correctly. The definition of a management system is from ISO 27001 [3]. The definition of security governance, governing body, top management, organization, and entity is from ISO 27014 [2].

Management system
The organization shall establish, implement, maintain and continually improve an information security management system, including the processes needed and their interactions, in accordance with the requirements of this document [3].

Security Governance
The definition of governance of information security is the means by which an or-

ganization's governing body provides overall direction and control of activities that affect the security of an organization's information [2].

Governing body
Person or group of people who are accountable for the performance and conformance of the entity [2].

Well-functioning board
A well-functioning board is characterized by having the company's overall management, looking after its best interests and objectives, making the necessary decisions, and carrying out relevant supervision and control [1]

Entity
Organization and other bodies or parties [2].

Organization
That part of an entity which runs and manages an ISMS [2].

Top management
Person or group of people who directs and controls an organization at the highest level [2].

2.2 Laws and regulations

Several legislation sets precise requirements for management's responsibility toward information security and preventive security work. One of these is the Security Act. The Security Act must prevent, detect, and counter activities that threaten security [12]. The Security Act applies to state, county, and municipal enterprises, in addition to suppliers, that process security-graded information or control and process systems that are of critical importance for essential national functions [12].

The Security Act specifies groupings of values worthy of protection, such as information, information systems, objects and infrastructure, and personnel security. As the issue essentially deals with the evaluation process, it is explicitly Chapter 4 that deals with requirements for preventive security work, of which § 4-1 on security governance is most relevant. Nevertheless, it is worth mentioning that the other chapters included in the Security Act are what must be protected by governance [12].

§4-1: Security governance
The company's manager is responsible for the preventive security work. This must be part of the company's management system, of which the state of security in the company must be regularly checked. The business must also ensure that employees,

suppliers and contractors have a sufficient understanding of risk and security [12].

All businesses subject to the Security Act must ensure that employees, suppliers, and clients understand security and risk. Furthermore, the business security regulation is one of several regulations included in the Security Act, where the business security regulation is the most relevant [13]. The most pertinent sections mentioned in this regulation are defined under Chapter 2 on security governance:

§3: Security governance
A business that is covered by the Safety Act must establish a governance system for security. The system must ensure that the business meets the requirements given in or authorized by law [13].

§5: Security goals
It must be determined by a business how the requirements for a proper security level in the Security Act § 4-3 first paragraph, § 5-2 first paragraph, § 6-2 first paragraph and § 7-3 first paragraph are to be met and criteria for evaluating whether the requirements are met [13].

§9: Evaluation and practice
An enterprise must regularly carry out an evaluation of whether the requirement for a proper security level has been met and at least once a year evaluate whether the management system for security is suitable to ensure that the requirement is met, cf. § 5 [13].

According to the Security Act, paragraph 3 is aimed at the governance system for security, of which the governance system's responsibility is to follow up on security goals [12]. §5 further explains that security goals apply to all security areas in businesses requiring an adequate security level. Furthermore, paragraph 9 deals with evaluation and exercises where the security goals set must be regularly followed up and evaluated at least once by the senior management as to whether this is justifiable [13].

2.3 Standards and frameworks

International Organization for Standardization

International Organization for Standardization (ISO) is an international standardization organization that has developed standards for various sectors. ISO 27001 is an international standard that has been provided to set requirements for establishing, implementing, maintaining, and continuously improving a management system for information security. There are many advantages to using ISO 27001. First and foremost, an information security management system can preserve confidentiality, integrity, and availability of information by using a risk management process. Furthermore, using the framework can give stakeholders confidence through adequate management of risks [3].

While ISO 27001 is an international standard that describes requirements for management systems for information security, ISO 27014 describes how the board of an enterprise should relate to such management systems for information security. The international standard provides six overall goals of what the organization should focus on. Some of these focus areas are how a culture of Information Technology (IT) security can be created in the business, how measures must fit in line with the business's requirements and challenges, and how risk management related to IT is done along with risk management in general. Further on, ISO 27014 shows how to evaluate, direct, monitor, and communicate and what these concepts entail [2].

According to ISO27014, evaluate is the governance process that considers the current and forecast achievement of objectives based on current processes and planned changes and determines where any adjustments are required to optimize the achievement of strategic objectives in the future [2]. To perform the evaluation process, the entity's governing body should ensure that initiatives take relevant risks and opportunities into account. Furthermore, they should respond to information security and Information Security Management Systems (ISMS) measurements and reports by specifying and prioritizing required objectives in the context of each ISMS. In addition, the top management of each ISMS should ensure that information security adequately supports and sustains the entity's goals and submit new information security projects with significant impact to the governing body for approval [2].

The NIST Cyber Security Framework

The NIST Cyber Security Framework (CSF) is written by The National Institute of Standards and Technology (NIST). It provides help to businesses of all sizes to understand better, manage, and reduce their cyber security risk and protect their networks and data. [14].

The NIST CSF focuses on five elements to help entities manage and minimize cyber security risks [14]. These five elements are identify, protect, detect, respond, and recover. Furthermore, the five elements are subdivided into 22 categories (groups of cyber security outcomes) and 98 subcategories (security controls) [15]. There are many advantages to using this framework. Several businesses have the opportunity to make use of the security controls addressed in this framework and carry out benchmarking against this. A challenge with such benchmarking is that compliance is not measured against specific security goals in the business. Instead, risk assessments and measures are based on requirements according to this framework alone.

ITIL Framework

The Information Technology Infrastructure Library (ITIL) is a framework for delivering effective IT/digital solutions. The purpose of the framework is to help businesses achieve value. ITIL helps companies introduce service delivery systems and a common language to meet customer needs [16].

To achieve value, the risk and costs must be lower than the positive outcome resulting from the action.The costs and risks introduced by the act must outweigh the costs and risks removed from the business once they have established a sharing relationship. There must also be outcomes that are affected rather than what you get out of the relationship. All do not have to be smaller, but the total weight of cost, risk, and the affected result must be lower than the positive sides to create value [17].

NS 5814:2021 - Requirements for risk assessment

Risk assessment is a process which consists of planning, risk analysis and risk evaluation [18]. A risk assessment is all about identifying threats and unwanted incidents, analyze and evaluate risk, and identifying measurements in order to both prevent and reduce risk.

NS 5814:2021 Requirements for risk assessment, describes and provides requirements for risk assessment for different organizations to make decisions regarding measurements and choices of solutions in order to prevent risk [18]. It also set requirements for the elements that can be included in such a process. The standard may be used by both private and public organizations regardless of size. This also includes volunteer organizations.

NSM's Basic Principles for ICT Security

NSM's Basic Principles for ICT Security defines a set of principles and underlying measures to protect information systems (hardware, software and associated infrastructure), data and the services they offer against unauthorized access, damage or misuse. The advantage of using NSM's basic principles for ICT security is that its use should contribute to raising security competence and the level of security in Norwegian businesses. These are relevant for all Norwegian businesses, both in the public and private sectors [19].

Key Performance Indicators

According to Jaquith, Key Performance Indicators (KPIs) are financial and non-financial measures or metrics, which are monitored using Business Intelligence techniques and tied to an organization's strategy typically using concepts or techniques such as the Balanced Scorecard [20].

It is stated by the COBIT framework that KPIs, described as Performance Indicators, indicate whether goals are likely to be met [21]. These indicators can also be measured before the outcome is clear and, therefore, are called "lead indicators". This allows us to determine the effect of security decisions in advance. The COBIT framework further explains that KPIs indicates how well the process enable the goal to be reached [21].

The Institute of Internal Auditors

The governing body, management, and internal audit are the core elements that imply and are essential for good governance. The Three Lines Model, also known as the Three Lines of Defense, is a model developed by The Institute of Internal Auditors (IIA), which has gained popularity for organizing governance and risk management in organizations. The Three Lines Model outlines essential governance elements and provides guidelines on how to implement The Three Lines Model in different industries, focusing on accountability, actions, assurance, and advice [22]. Figure 2.1 shows the relationship between the three lines.

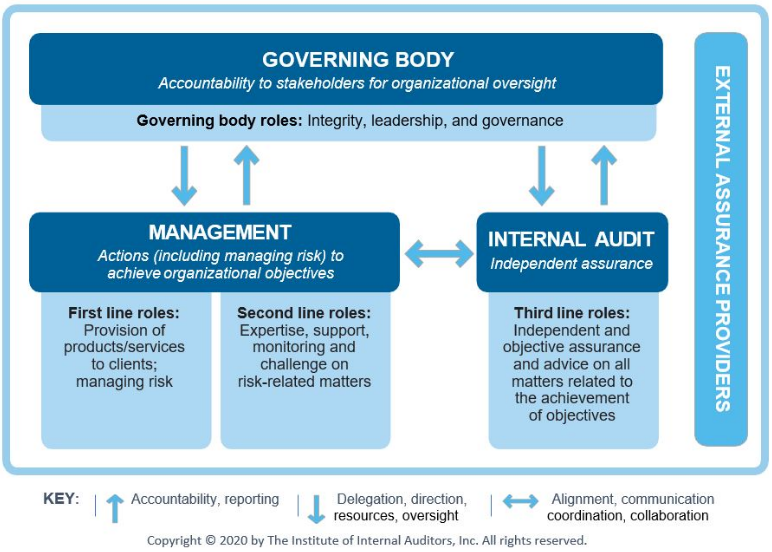
GOVERNING BODY
Accountability to stakeholders for organizational oversight
Governing body roles: Integrity, leadership, and governance
MANAGEMENT
Actions (including managing risk) to achieve organizational objectives
INTERNAL AUDIT
Independent assurance
First line roles: Provision of products/services to clients; managing risk
Second line roles: Expertise, support, monitoring and challenge on risk-related matters
Third line roles: Independent and objective assurance and advice on all matters related to the achievement of objectives
EXTERNAL ASSURANCE PROVIDERS
KEY:
Accountability, reporting
Delegation, direction, resources, oversight
Alignment, communication coordination, collaboration
Copyright © 2020 by The Institute of Internal Auditors, Inc. All rights reserved.

Figure 2.1: The Three Lines Model. Copyright with permission by The Institute of Internal Auditors [22]

.

2.4 Articles and reports

Mørketallsundersøkelsen

In 2022, Næringslivets Sikkerhetssråd, created the 13th ‘Mørketallsundersøkelsen´. The survey maps the IT industry and examines the extent of computer crime, security incidents, and security awareness among Norwegian businesses [23]. Mørketallsundersøkelsen is carried out every other year, and in the survey from 2022, this was expanded by 1,000 respondents to ensure a better statistical basis.

In the survey from 2022, it is mapped that half of the businesses that have responded have a framework or a governance system for information security [23]. Compared to the previous surveys, this is now at a level with 2016 and 2018, but somewhat lower than in 2020. In 2016 and 2018 this was around 50%, while in 2020 this was over 60%. Here it is also pointed out that large companies have frameworks to a greater extent than small companies. This information gives an indication of what can be combined from the answers from the interviewees, and provide guidance for the thesis’ hypothesis.

Styreboken

According to ISO 27014, it is required for both members of the governing body and managers to fulfill their respective roles consistently to achieve effective governance of information security [2]. According to ‘Styreboken´ published by PWC, an important aspect of the governing body is its responsibility to ensure that the information security management understands and responds to changes, risks, and opportunities, enquire that new business opportunities are considered and that adequate risk-reducing measures are implemented [1]. It is also imperative that the governing body works purposefully and ensures that businesses set ambitions, create results, and report on target achievement.

Furthermore, a well-functioning board is characterized by its overall management of the entity, ensures the company’s best interests and purposes, performs necessary decisions, and carries out appropriate supervision and control [1]. The governing body’s role and responsibilities will change along with the entity’s development and the environment. Creating and visualizing values for the owners is an essential and central task for the board. Gaining a better understanding of what the most critical risks entail, how these affect the businesses as well as how these are to be handled will be an important element for the board. It is also essential for the board to understand how different risks will affect value creation and results within the entity, ensuring an active perspective regarding risk profile and risk tolerance.

Governing and control are both important, in addition to the organizational tasks, the management responsibility, and last but not least, the strategy work where all is necessary to contribute to the entity's development. The work with sustainability, reporting, and supervisory responsibility are all tasks that are part of the governing body and require their immediate attention. Also, recurring areas with a continuous need for learning and development, such as internal control and risk management, are important tasks that the governing body must manage [1].

2.5 State-of-the-art analysis

To what extent are management systems known and used?

After the release of ISO 27014 in 2013, it was provided a report by Mahncke on how the standard can be applied to Australian general medical practice [24]. After all, the standard applies to organizations of all sizes. As a result, it was confirmed that the governance component of information security required support in the form of standards. However, developing a security culture is crucial to good governance in medical information security.

According to Brand et al., due to an increasing trend worldwide of enterprise mobility, several risks originate from using mobile devices for business-related tasks [6]. Based on information technology governance frameworks, the study provides 12 practices companies can employ to mitigate these risks. One of these frameworks is ISO 27014. The 12 practices in this survey aim to increase efficiency and provide an effective solution to govern enterprise mobility security risks, as the frameworks alone can be generic and inefficient. The study states the importance of establishing and implementing security governance frameworks in an organization [6].

Due to increased attacks targeting financial institutions, Al Batayneh et al. provided a research article resulting in a scoring model that could predict the adequacy of an information security governance framework for a bank [7]. A novel method for scoring information security governance frameworks was introduced to assess their adequacy without implementing it. In this way, financial institutions could evaluate the effect of implementing an information security governance framework before implementing it. With an accuracy of 75%, the survey using the scoring model could conclude that the adequacy of an information security governance framework was sufficient [7].

What is used to evaluate the state of security and to what extent is this a justified state?

According to Zia, it is crucial to acknowledge the value and importance of information security and set directions to develop an information security environment

[25]. Furthermore, it is stated that information technology security governance has become a fundamental function. Still, the management executives do not understand the risks associated with information security governance. ISO 27014 is one of the frameworks used to determine the capability level of organizations surveyed, resulting in most respondents describing their implementation of information technology security governance at low capability levels [25].

According to Maynard et al., some of the activities involved in security governance are explained [26]. These activities include, among others, adjusting organizational structures, designating roles and responsibilities, allocating resources, managing risks, measuring results, and gauging the adequacy of audits and reviews. The article further explains how information security governance influences the quality of strategic decision-making to ensure that investments in security are effective [26].

Which roles are involved in evaluating security performance?

According to Von Solms, it is explained how important it is for the governance board to maintain the protection of the organization's information and assets [27]. It is further mentioned that this protection is only achieved through effective management and effective board oversight. The board needs to expand these directives into policies, company standards, and procedures to provide strategic direction and guidance in how an enterprise should operate. Also, the board must ensure compliance with national laws and regulations and all organizational directives, policies, company standards, and procedures defined to claim the board has 'control over its affairs' [27].

According to Maynard et al., the case study focuses on an Australian private company organization where the decision-making is delegated to the division level. However, the information technology manager is responsible for all security in the organization, including security governance. Furthermore, the company's organizational structure consists of a private ownership board, a management committee comprising the CEO, CFO, and department heads, and a business division comprising finance, IT services, human resources, etc., [26].

According to Da Veiga and Eloff, the board's responsibility is to effectively direct and control an organization through reasonable leadership efforts [5]. Furthermore, it is stated that the management and board are responsible for developing and distributing corporate codes of conduct. To deploy an information security strategy in an organization, the security leadership highlights the importance of an executive-level security representative. Lastly, the responsible executives shall communicate the right information security culture, frameworks, and acceptable information security behavior.

What is needed to reduce the uncertainty surrounding the state of security?

According to Ahmad et al., due to digitalization at an alarming speed, information security risks in enterprises are increasing with a significant impact [28]. Furthermore, due to several security breaches among businesses, awareness amongst the board of directors and the executive management has increased, and the importance of creating an oversight function to review, monitor and govern information security. By incorporating the knowledge on information security governance identified in practice and academic literature along with associated information security domains, an information security governance process model for financial organizations is further developed and provided. The five proposed information security governance processes are monitor, direct, evaluate, communicate, and assure [28].

According to Da Veiga and Eloff, the behavior of employees must be directed and monitored to achieve compliance with the security requirements [5]. It is further stated that before employees can adhere to and exhibit an acceptable level of information security culture, the management needs to implement and communicate specific security controls.

According to Salmenpää, civil aviation is a continuously evolving ecosystem in which information security plays an essential role in ensuring public and societal trust as well as confidence in civil aviation [29]. Furthermore, it is stated that governance plays a key role in finding sustainable, coherent, and holistic ways to implement information security through the complete civil aviation ecosystem. The study focuses on understanding the objectives of information security governance by following the strategies given in ISO 27014. At last, it is stated that the meaning and purposes of information security governance should be better recognized and understood as it is crucial for efficient performance and risk-based information security [29].

The study provided by Huang et al. provides a method to integrate information security management systems (ISMS) with information security governance [30]. This is due to the reason that ISMS policies need a connection to the strategic risk management of organizations. Furthermore, it is stated that if there is no perception of information security management in mind and no information security governance is embraced, information security technology cannot be recognized, and a well-performed ISMS cannot be accomplished [30].

2.5.1 Summary of state-of-the-art analysis

The related work aligned with the first research question is mainly based on the importance of providing effective solutions to govern and mitigate risks by introducing security governance frameworks in an organization. Furthermore, one article in particular points out ISO 27014 as highly relevant. However, it is no mention of the actual use of governance frameworks, in particular ISO 27014, among the articles. Regarding the second research question, no specific sources are mentioned other than the importance of protecting the organization's information assets.

One of the previous articles states that the roles and responsibilities of information security are aligned with the management and the governing body. There is no mention of which roles are involved in evaluating the security condition. However, considering the fourth research question, the importance of culture, competence, and maturity is highlighted as a whole by all previous studies.

Several essential and relevant insights emerged during the literature review. Still, the previous related work does not examine the different research questions in-depth, how organizations work with evaluation as an element of their security governance, and what potential lies within this process to ensure effective management and control of the organization's security level and compliance. Nor does the previous work examine how the evaluation process can provide value, become more efficient, and ensure that the basis for governance and control is better. In contrast, this master thesis will to a greater extent, examine the key elements listed above.

Chapter 3

Methodology

The methodology chapter is a description of what has been done and all the choices made during this master thesis. The first choice of method deals with qualitative or quantitative analysis. Furthermore, the choices made regarding the structure of the interview guide are described, before the selection and the recruitment of interviewees is described. Finally, the implementation is discussed of the interviews and then the analysis. Figure 3.1 shows a flow chart of the different steps of the research process. The first step of this research study was to choose which research method to use. Before the data is analyzed, the next step is the planning, recruitment, and execution of the interviews. As data analysis was performed during the interview process, both interview process and data analysis are marked as an iterative process. The last step describes the results.

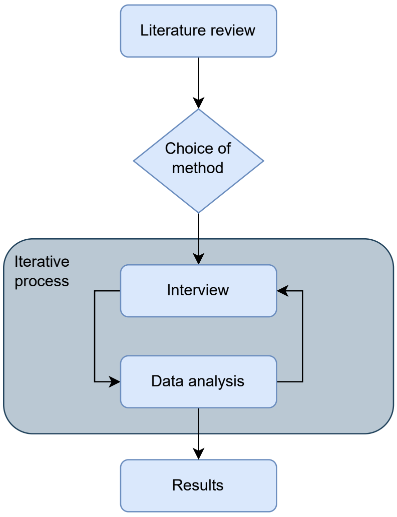

Figure 3.1: Flow chart of the research process

Alternative methods, tools and the like will be listed, of which the applied methods will be justified and why other methods were not chosen. The book ‘Practical Research: planning and design´ by Leedy and Ormrod, is the primary source used of the choice of methods and applied method of the problem description addressed in this study [31]. The book elaborates on strategies in research methodologies and provides relevant and updated information regarding methodologies such as qualitative and quantitative methodologies. The book 'Kvalitative forskningsmetoder: I praksis´ by Tjora, is also used as the book elaborates qualitative research practice through a number of examples and also reflects on the potential of this research [32]. Techniques for data generation, such as observation, interview, document studies, use of the Internet and several others is both presented and discussed [31, 32].

3.1 Choice of methodology

The first choice of method is to decide between qualitative and quantitative research methods. The advantage of using a quantitative research method would be to get a more generalized result that can describe a situation as it is [31]. However, the qualitative research method is more suitable because it is desirable to create a more in-depth knowledge of a specific area that entails what led to certain decisions and what thoughts are used as the basis for various choices made. According to Leedy and Ormrod in the book "Practical Research: planning and design", another benefit of using the qualitative method is the iterative process which allows the researcher to move back and forth between data collection and data analysis [31]. This may benefit the project by using the knowledge obtained from the first data subjects to gather even more relevant information from the later data subjects. In contrast, the quantitative method often follows a waterfall model, where data collection comes first and then the data analysis afterward [31].

Carrying out analysis of collected data can be done in several ways. Qualitative research yields mainly unstructured text-based data such as interview transcripts and observation notes [33]. The data analysis must be done systematically by searching and arranging the interview transcripts to increase the understanding of the phenomenon. This process involves coding or categorizing the data. An alternative is to manually code the responses into Microsoft Excel by extracting the essence of each answer and entering this into a form. A disadvantage of this method is that it is time-consuming, and additional comments to the various questions are not included.

Another option is to use a tool to analyze qualitative surveys more easily. An example of such a tool is NVivo[33–36]. An advantage of this tool is the ability to conduct the analysis and coding of the data basis more efficiently and conduct searches in the data, for example, what a given business answered on a given question. Another well-known tool is ATLAS.ti [37]. ATLAS.ti is also a tool related to qualitative research that can be used to code and analyze transcripts, build literature reviews, and create network diagrams. Nevertheless, setting aside time to become well acquainted with the tool's use and possibilities is essential. Whether the tool's data processing and privacy policy align with the set requirements for the collected data must also be carefully checked.

Limitations

As the method should be decided based on what type of information is needed, the requirements and limitations of the research study must be considered. The data acquired must provide insight into the focused area of this research to know what needs further investigation. In Chapter 1, the problem description describes a knowledge and a communication gap in digital security and the aligned consequences.It is essential to understand previous knowledge and information on the topic and identify gaps. To provide further knowledge in this area, the focus of this research study is to gather previous knowledge and information on the topic.

The main limitations for this master thesis are both time and resources. The time frame given for this master thesis is set from January until June, where only one person will be writing and providing the study as the master thesis is individual work. Furthermore, interview objects must be gathered as a part of the research process. As the number of interview objects depends on the number of both companies and controlling authorities contacted, this can also be considered another limitation of this master thesis.

Qualitative research design options

According to Leedy and Ormrod, five commonly used design methods exist for qualitative research [31]. As there are several options, it is important to choose the research design that is best suited for the task and will yield the most benefit. The first is a case study, also known as idiographic research, which focuses on an individual or situation studied in depth over time. The benefit of case studies is to better understand a poorly understood situation, for example, mapping dependencies of the evaluation process amongst companies. The second research design is ethnography. Unlike the case study, the researcher focuses on an entire group, often for a longer period, often several months or years [31, 32]. As the focus of this master thesis is not aimed at examining the behaviors or beliefs of the companies, this research design is, therefore, unsuitable.

The third qualitative research design introduced is the phenomenological study, which aims to understand an experience from the participant's point of view. The researcher works with the participants through unstructured interviews to find the answers. Grounded theory study is the fourth research design where this study aims to derive a theory from the data collected in a natural setting. This can be considered a fitting research design when existing theories are lacking or inadequate. The final qualitative research design is a content analysis that examines forms of human communication such as books, journals, music, films, and more to identify patterns, themes, or biases. A content analysis aims to identify the specific characteristics of a body of material.

Chosen method

To answer the research questions described in section 1.5, a case study is the chosen method as a case study can use interviews and relevant documents to understand a situation in depth [31, 32]. The structured characteristic of the interviews can be helpful to answer all five research questions, as the goal is to answer many specific questions in which the researcher predetermines. Furthermore, it will be possible to create an even clearer thematic focus, and at the same time a more standardized and predictable progress in the interview.

3.2 Applied method

Scoping Literature Review

According to Peters et al, a scoping review consists of a broader approach that aims to clarify previous concepts and identify knowledge gaps [38]. Scoping reviews can be beneficial when the area of study is emerging as they are suited to reduce the research questions and problem descriptions after the gaps are identified [39]. According to Arskey and O'Malley, depending on the purpose of the review determines to what extent the in-depth coverage of available literature is needed [40]. Furthermore, Arskey and O'Malley provide four reasons to undertake a scoping literature review, where the fourth reason aims to identify gaps in the existing literature.

The main search engines and databases used when searching for relevant online sources are listed in Table 3.1. The literature review began before the master thesis itself, where the retrieval of the literature review has been an ongoing process and lasted until April 2023. In addition, to identify relevant research projects and studies, it was important to determine suitable keywords to scope the different results. The main keywords used to obtain a comprehensive basis for literature in this thesis are the following: *ISO 27014 governance processes, evaluation process, management system, security board, and security governance*.

Interview planning

According to Leedy and Ormrod, it is essential to determine the interview questions in advance [31]. Furthermore, it is stated that the questions must be related

Search engines
ACM Digital Library
Elicit
IEEE
Oria
Google Scholar

Table 3.1: Search engines used to conduct literature review

to the research questions to make the analysis easier. In order to be successful with the interview situation, an important prerequisite is to manage to create a relaxed atmosphere where the informant feels comfortable. Furthermore, it is important that the interviewer has a clear and distinct framework for the interview, where the informants often have expectations that the interviewer is in charge, with concrete, defined questions, to which the informant answers relatively briefly and precisely.

Interview guide

To conduct an interview guide, Leedy and Ormrod introduce examples of how to align the interview questions with the research questions and the overall research problem [31]. In other words, the first step in preparing the interviews was to decide on the research questions. Table 3.2 show the research questions aligned with the interview questions. Furthermore, the interview questions were assigned five different categories. Each category was designed based on the research questions in section 1.5.

The interview guide was designed and made in collaboration with an experienced security governance professional. Furthermore, as only Norwegian businesses and controlling authorities will be interviewed in this survey, it is considered most appropriate to design the interview guide in Norwegian. In the interview guide, each question was linked to theory and purpose. The theory helps to give the analysis a professional basis and make conclusions more realistic. The purpose provides guidelines for the analysis and describes points of comparison that are important to emphasize.

Recruitment

After the interview questions were determined, relevant participants were contacted. According to Leedy and Ormrod, the book elaborates on the importance of including informants who can express themselves reflectively about the topic in question [31]. Therefore, it is important to scope the interview participants. As the problem description focuses on the evaluation process, it was desirable to gather participants either responsible for it or a representative of the governing

Research question	Interview question
1. To what extent are management systems known and used?	Does the entity have a given definition of security governance? Does the entity have a given definition of management system? Does the entity have a system and/or framework for management systems? Is the entity familiar with the processes addressed in ISO 27014, or does the entity use other defined processes for governing?
2. What is used to evaluate the state of security and to what extent is this a justified state?	How does the entity operate with the evaluation process and what is involved in this process? What is the data basis used to evaluate the state of security? Does the company use any tool to secure data basis and assess the effects of activities and measures? Does the entity have a process for deviation reporting that forms basis for evaluation? Does the entity have a process for risk reporting that forms basis for evaluation?
3. Which roles are involved in evaluating security?	Where/in what role has the entity placed responsibility for evaluating the security condition? What role does the board have in security governance? Who has the responsibility for the dialogue with the board of the entity? Does the entity use other control functions, in addition to CISO, to follow up the evaluation process?
4. What is needed to reduce the uncertainty surrounding the state of security?	Has the entity an overview of the values and their respective criticality? Has the entity any goals set for information security? Does the entity use indicators for goal achievement? Has the entity set requirements for which evaluations will be carried out in different parts of the organization?
5. Is there a correspondence between the supervisory authorities' experiences and the companies answers?	All questions asked.

Table 3.2: Research question aligned with interview questions

body.

Execution of the interviews

An email was sent out to the carefully selected businesses with basic information about the topic, goal, and interview duration. The time frame for each interview was set to be between 45-60 minutes. The main medium used to perform the interviews was Microsoft Teams, but some were conducted both physically and over the phone in cases where the participant preferred this. Most of the interviews were executed with either one or two participants, often including the CISO and/or CSO and the head of cyber security governance.

In advance of the first interview, preparations were made in the form of an interview guide to detect any errors or deficiencies. Corrections and improvements were carried out both before and during the interview process. The timetable for carrying out the interview was set at one month. This was calculated as more than enough time to complete all the interviews so that enough time was set aside afterward to carry out and process the analysis. The interviews were tried to be set up as early in March as possible. Therefore most of the interviews were carried out early this month, but some interviewees did not have the opportunity until later this month, and a couple of interviews were thus set up in the last week of March.

Before the interview, the participant was sent both a data processing form and an interview guide. The data processing form is a document that describes what the information from the interviews will be used for and how this information will be processed. Both parties must sign the document and a checkbox for whether the business wishes to be anonymous, of which the undersigned is obliged not to violate this wish. The interview guide includes all the questions to be asked during the interview. This document was sent in advance so the participants could prepare if they wanted. The data processing form is attached in Appendix A. The interview guide is attached in Appendix B.

Data Analysis

The chosen method for the data analysis is Creswell's data analysis spiral. According to Leedy and Ormrod, Creswell's data analysis spiral can be particularly useful as it is suitable for qualitative analysis and focuses on how qualitative data analysis can reasonably be proceeded [31]. As qualitative analysis is an iterative process, and the researcher has the opportunity to move back and forth between the processes, the researcher must eventually move forward, leaving earlier ones behind. Cresswell's approach consists of four steps. Each step can be gone through repeatedly until the data analysis is complete.

The first step consists of organizing the data which suits the project. In this project, NVivo, a qualitative analysis tool, has been used as this tool is available for all NTNU students [34]. Furthermore, the benefit of using NVivo is the possibility of removing the tremendous amount of manual tasks. It allows more time to investigate trends, identify themes, and make conclusions [34, 35]. Reports from each interview were uploaded as a separate one to Nvivo as software. A code was created for each question, where each answer was linked to the corresponding code. Furthermore, a class was created from each file, of which these were classified as interviewees. For each interviewee, one attribute was set, a sector.

The second step is to peruse the entire data set several times to determine potential categories. Furthermore, the third step aims to identify categories and find meaning in the data. The last process focuses on the integrated and summarized data as a whole. Due to the given time frame of this master thesis and to ensure the progress needed, the data analysis was performed during the data collection process. In other words, Cresswell's data analysis spiral was performed with the current data available and was further repeated when newly added data was retrieved.

Chapter 4

Interview guide

In this chapter, the interview guide, which lays the foundation of the research project, is described. The interview guide consists of five categories, each dealing with different areas to form an overall picture of each enterprise. The questions mainly center on the evaluation process, framework conditions, values, objectives, and organization.

There is a minor difference between the two interview guides provided. The interview guide used to interview the controlling authorities directs the questions about their experiences on how companies relate to information security governance. On the other hand, the interview guide used to interview the companies asks directly what is done and how the different businesses operate with information security governance. The entire interview guide associated with companies is in Appendix B. The complete interview guide associated with controlling authorities is in Appendix C.

4.1 Category 1: Framework conditions and requirements

The first category deals with various businesses' framework conditions and requirements to support compliance. The emphasis focuses on frameworks and processes, statutory requirements for evaluation, and the board's responsibility for security. In this category, there are questions with frameworks as a theoretical basis to map the use of frameworks and the possible effect of this. These frameworks are described in Chapter 2.

The purpose of the questions included in this category is, among other things, to investigate the various definitions used and to determine whether there is a common agreement on what both a management system and security governance are and entail. Furthermore, it is desirable to see whether the use of a system or a framework for management has anything to say about how the company manages, including looking at whether those who use a system/framework carry out governance in the business more efficiently. It will also be examined to what extent the companies work process-oriented with security governance.

4.2 Category 2: Goals and values

Category 2 will examine how businesses evaluate security against the company's values and goals. The questions in this category aim to investigate and assess the basis for the board's commitment and ability to manage and thus indicate the evaluation process's importance. An example of such a question is whether the company has an overview of its values and their aligned criticality.

The theory used in this category is primarily statutory requirements, such as the Security Act, and best practices for mapping, assessing and safeguarding national security interests, societal functions, and other interests and values in various industries and sectors [12].

4.3 Category 3: Organization

The organization is a category that examines the organization in the business, which directly focuses on who does what and how they do it. The theory for these questions mainly covers best practices and white papers, such as ISO 27014 and The Three Lines Model [2, 22].

The questions' purpose is to map and identify the organization and placement of various roles. Among these, it is desirable to examine and identify the impact of the location of different control functions, the location of evaluation responsibility, and the location of security responsibility on the board's commitment. Investigating how the company works with the basis for management's review in this category is also appropriate.

4.4 Category 4: The evaluation process

The fourth category deals with the evaluation process and examines whether the goals set in the business have been achieved and/or are possible. The theories related to these questions are based on standards, legislation, and best practice such as ISO 27014 [2].

The purpose of the questions in this category is to determine what forms the basis for the evaluation and how the evaluation process is carried out. It will also be investigated which stakeholders are directly involved in the basis for the dialogue with the board and uncover different areas of responsibility in the company regarding the evaluation process. Access to relevant tools for evaluating and reporting the security condition would also be appropriate to request in this category.

4.5 Category 5: The relationship with the board

The relationship with the board is the last category, with a few questions to investigate and map the dialogue between the board and the security management. This section's theory is based on best practices and relevant articles, such as 'Styreboken´ published by PWC [1].

The purpose of the questions asked in this category is to investigate various processes and solutions to ensure the board's involvement, interest, and understanding of its role concerning security management, as well as the extent to which the board is actively involved in determining the direction and evaluating the effects of investments and measures. Questions are asked about the board's role in security management, who has the dialogue with the board, and how the evaluation process is followed up with the board.

Chapter 5

Results

This chapter elaborates on the responses from the survey and examines how these can answer the research questions. How this relates to previous findings and work will be discussed in Chapter 6. To answer the research questions, only a selection of the interview questions will be analyzed as this selection was revealed to be the most important to answer the research questions addressed in section 1.5. However, access to all the answers provided by the companies can be found in Appendix D and all answers provided by the controlling authorities in Appendix E.

5.1 Demographics

A total of two sectors have been analyzed, the private and public sectors. Within the private sector, the businesses are distributed and cover the financial, consulting, power, energy, and industrial sectors. In the public sector, businesses are distributed and cover the transport, administration, and power and energy sectors. A total of 14 companies were interviewed in this survey. Furthermore, all companies are anonymized.

All businesses correspond to large companies in both the public and private sectors. All 14 enterprises have over 100 employees and are defined as large enterprises by NHO [41]. Nevertheless, the size of the large enterprises varies greatly, with some having a couple of hundred employees and others having several thousand.

	10.000+	**1000+**	**100+**	**Sum**
Public	2	3	2	7
Private	3	2	2	7
Sum	5	5	4	14

Table 5.1: Frequency table: Companies

A total of four controlling authorities have been interviewed in this survey. On one or more occasions, the controlling authorities in this survey have supervised the businesses interviewed in this thesis. Furthermore, the controlling authorities are anonymized.

	Quantity
Controlling authorities	4
Sum	4

Table 5.2: Frequency table: Controlling authorities

5.2 To what extent are management systems known and used?

According to the description of security governance given in ISO 27014, very few companies know this definition, and even fewer use it. In the public and private sectors, only two companies, one from each sector, have defined both a management system and security governance. Furthermore, one business in the private sector has defined a management system but has no clear definition of security governance. The remaining companies in both public and private sectors explain that although there is a lack of a clear definition of a management system and security governance, the concept is incorporated through policy and awareness activities.

A total of nine enterprises use ISO 27001 in whole or in part. Of these companies, only a couple are ISO 27001 certified. The businesses in the public sector use frameworks based on, among other things, NIST, NSM's Basic Principles for ICT security, and the ISO family, where ISO 27001 is mentioned by four businesses specifically. Only one company within the public sector makes use of the ISO 27014 framework and uses it actively. Businesses in the private sector also use frameworks based on NSM's Basic Principles for ICT Security, ISO 27001/27002, and NIST, where two companies specifically mention the NIST Cybersecurity Framework. Figure 5.1 only shows frameworks the businesses have mentioned and not all they necessarily use.

Only a few companies are aware of ISO 27014 and the governance processes addressed in this framework, and even fewer use them. According to ISO 27014, direct, monitor, evaluate, and communicate are governance processes governing the performance of the management system. In the public sector, only one business actively uses these processes. In the private sector, only one company knows the governance processes mentioned above and desires to introduce these in the industry. The remaining companies in the public and private sectors either have

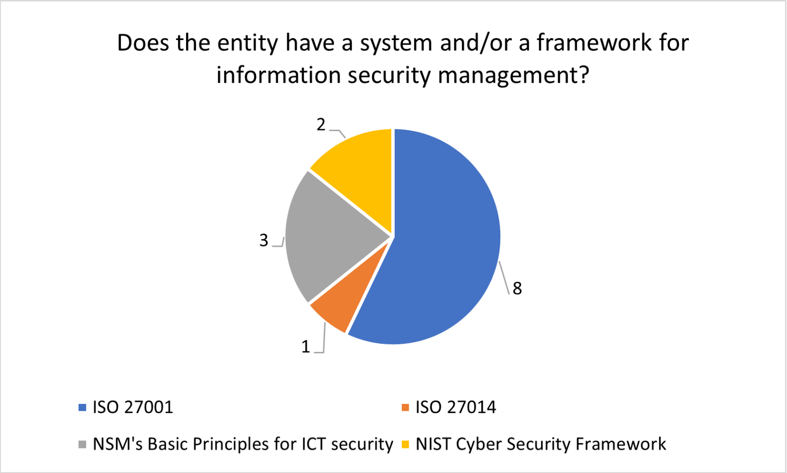

Figure 5.1: Question: Does the entity have a system and/or a framework for information security management?

little or no knowledge of or use the governance processes addressed in the ISO 27014 framework.

Many companies examined in this survey carry out evaluations but not by the governance processes addressed in ISO 27014. Identify, protect, detect, respond, and recover are processes included in the NIST CSF framework where there are two businesses in the private sector that make use of these processes for annual evaluation. Most of the remaining companies in both public and private sectors do not relate to any specific processes other than the elements included in the Plan, Do, Check, Act (PDCA) cycle.

5.3 What is used to evaluate the state of security and to what extent is this a justified state?

Two companies in the public sector describe the evaluation process where goal achievement is assessed and whether this was good enough or whether these goals need to be adjusted or corrected. It is further explained that the elements included in this process are information that has been collected through functions, conversations with support functions, collaboration with IT, follow-up of control activities, etc. This is then collected in forms, and professional assessments are made of what is also discussed with the management line and whether it requires changes or the various identifications create potential. Another company explains that the elements included in the evaluation process are unknown. Still, information security control and evaluation are carried out, as well as internal control, technical vulnerability tests, risk assessments, and more. This business also points out the evaluation process as an area for improvement. In addition, three other companies claim that the evaluation process is unclear and unsystematic. The last company performs the evaluation process at several levels, where reports and corrections are carried out if deviations are detected.

In the private sector, three companies informed that the evaluation process takes place in the management's review. It is further stated that certain evaluation criteria must be made in various business areas where maturity, challenges, and proposed measures are described. This must also be assessed concerning the general risk and threat picture of what should be emphasized. Another company explains that they use a framework in the evaluation process to follow up the goals set and given by the same framework, the NIST CSF. This is carried out in workshops where spreadsheets are used for mapping and evaluation. Furthermore, another company explains that previously no work has been done with the evaluation process and that this has taken place minimally but will now be improved. The last business informs that they have not defined an evaluation process but a GAP analysis against NSM's Basic Principles for ICT security, where follow-up and prioritization are carried out.

Businesses in the private and public sectors explain that they have performed an appraisal. It is essentially an overall valuation of the company's values, where the most vulnerable and critical values have acquired criticality. Almost all businesses in both the public and private sectors explain the degree of difficulty surrounding the value chains and their mapping. Nevertheless, some companies respond that the general and overall value assessment made in their business is good.

Most businesses, in total, have set goals for information security. Still, there is some variation between the companies as to whether these goals are at an overall or more profound level. Six out of seven public sector enterprises have set information security goals. The one business in the public sector, which also uses the ISO 27014 framework, uses one of the governance processes 'direct,´ which the business calls 'goals and performance management,´ where they have long-term, strategic goals that are broken down into operational goals which is revised annually. Another company in the public sector informs that they have a stated goal for information security and the Confidentiality, Integrity, and Availability (CIA) triangle, but this is not quantitative enough to evaluate or measure.

In the private sector, all the companies have set goals for information security. Over half of the companies in the private sector have overarching goals, most of which mention that these are in their policy for information security. In contrast, only three companies have goals elaborated in their corresponding underlying policies. One of these three companies mentions that their security goals are organized according to the NIST CSF. Furthermore, another company informs that its security goals are linked to establishing controls, which are integrated into its so-called risk management.

In both public and private sectors, it is common for most companies to use Key Performance Indicators (KPIs) to measure the effects and possible measurements determine whether the set goals for information security have been achieved or are possible in the business. Furthermore, it is informed that these KPIs are used to a certain extent, as only some goals are equally measurable in the individual business. In the public sector, a company elaborates that information is obtained through the monitor and evaluate process where they carry out information retrieval/control. Furthermore, a self-assessment of the state of security of the various areas within the businesses is carried out, which is reported as a part of business report to the security management, where a new assessment is made based on whether something has been achieved or not. In the private sector, three businesses explicitly mention that, in addition to established KPIs at the group level, various processes are used to measure and monitor whether the goals are achieved using a framework. NSM's Basic Principles for ICT Security and NIST CSF are particularly emphasized here. Furthermore, two businesses in the private sector use maturity measurement according to ISO 27002.

Two companies, one from each sector, do not have a process for non-conformity reporting that forms part of the basis for evaluating the state of security. The one business in the public sector this applies to specifies that this is a conscious choice made by their tech department. To which this also applies, one company in the private sector responded that they have technology that can extract this. On the other hand, all businesses have a process for risk reporting which forms part of the basis for evaluating security efficiency. Only one company in the private sector answers that they could be more decisive in risk management, both in terms of operational and security risk. The company further explains that several adjustments are needed in the governance. There are no requirements for how risk should be assessed, where it should be assessed, and how it should be reported, handled, and aggregated. Figure 5.2 shows which processes and/or tools the different companies use to evaluate the state of security, and not all they necessarily use.

5.4 Which roles are involved in evaluating security performance?

The responsibility for evaluating the state of security and achieving goals applies and varies between the businesses in the public sector. Two companies inform that this responsibility lies at the group level with the Chief Executive Officer (CEO), which further delegates down the hierarchy. Two other companies explain that the responsibility lies with the Chief Information Security Officer (CISO), whereas one company specifies that this is done in collaboration with the CSO, where both

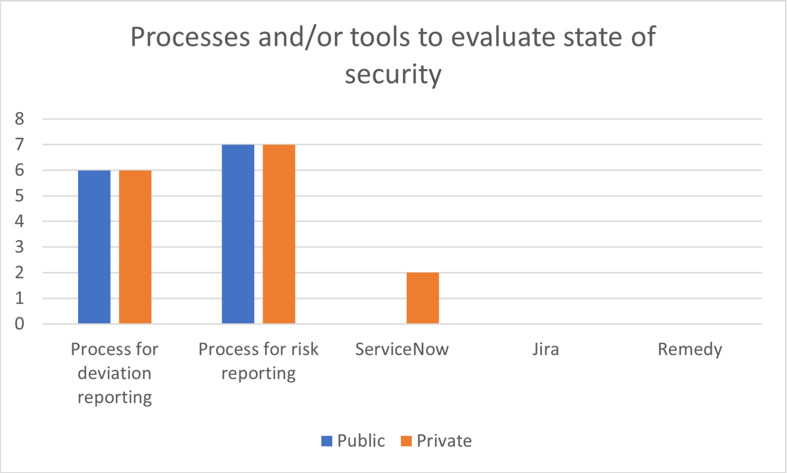

Figure 5.2: Processes and/or tools to evaluate state of security

participate in a comprehensive report of all security areas. Furthermore, another business informs that they have an overarching policy that the Chief Security Officer (CSO) has for all its management systems that set requirements for everyone. Within everyone, there will be concrete goals that will be defined, and they will be anchored with the business strategy, and all must decide on this. The last two companies inform that the responsibility lies with the security manager and the security section. Only one company explains that they are working to incorporate the evaluation at each departmental level to understand their security situation better.

In the private sector, five companies inform that the responsibility for evaluating the state of security and goal achievement lies primarily with the CISO at the group level. In addition, one business specifies that this responsibility is shared with the Security Manager in the business area. Furthermore, another company in the private sector explains that responsibility is placed in the first line. They further explain that the second line can evaluate the first line's evaluation. Still, it is not the second line that actually evaluates the state of security and goal achievement. The last company informs that the responsibility lies with the CEO's office. Figure 5.3 shows an overview of the different responsibilities among the companies.

Two enterprises in the public sector explain that they use CSO as a control function, in addition to the CISO, to follow up on the status and basis for evaluation. Another business explains that they use the group audit as a third line. Furthermore, another company explains that security coordinators are in the line, i.e., in counties and business areas. These are called support functions that look after and report to the security management if they see errors and deficiencies that need to be followed up. The company also has a function in IT called digital se-

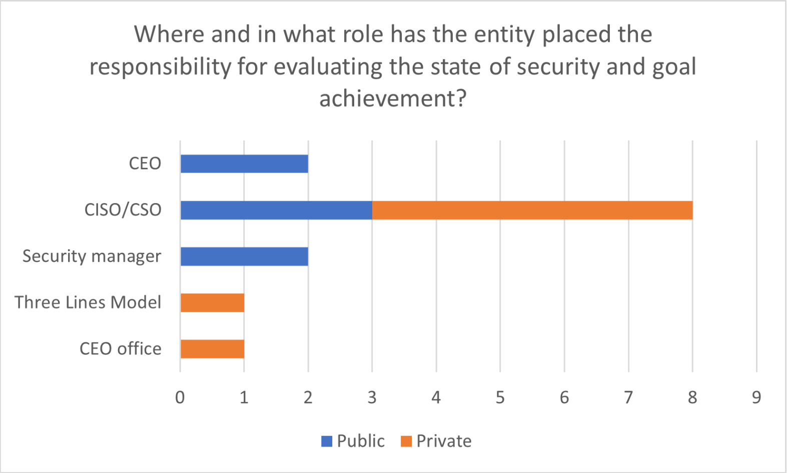

Figure 5.3: Question: Where and in what role has the entity placed the responsibility for evaluating the state of security and goal achievement?

curity which follows up more technical security. Another business informs that they use data protection representatives and external audits. The latter company replies that they use risk management and internal control functions to achieve input and support to security management.

In the private sector, five businesses mainly use internal and external audits as control functions, in addition to the CISO, to follow up on the status and basis for evaluation. Another company explains that they use a Data Protection Officer (DPO) who will, from their point of view, evaluate security related to privacy regulations. The latter company informs that they do not use control functions other than the CISO to follow up on the status and basis for evaluation.

Six companies in the public sector answer that it is mainly those with professional responsibility for security who participate in evaluating the status before management's review, where a report is drawn up which is anchored by those responsible for it. One of these six businesses further informs that the risk management function will also be involved. Of the participants included in the management review at the top level, six companies answered that this mainly consists of group management and top management in addition to CISO/CSO. It is also mentioned by some specific businesses in the public sector that the CEO participates in management's review.

In the private sector, one business explains that their enterprise risk management is reported to the corporate management board (CMB) through a written note and a presentation. This is reported from the management to the board. The business further informs that they have a governance committee where the CEO agrees on what is desirable to report across the business areas. Both CEO and CISO attend the group management, supporting the management's review. The remaining six businesses in the private sector also inform that the CISO and the top management participate in the management's review at the highest level. Only a couple of companies in the private sector further inform board members who participate in the management review.

Two companies in the public sector inform that there is a close dialogue with the assignment letter. Here, one of the two businesses further declares that the board is engaged and gives an annual assignment to follow up with dialogue and reports for each term to ensure compliance with the Security Act. Three businesses explain that the board's role in security management is mainly based on their role as supervisor, where they must ensure that the business is in line with the guidelines and set speed and direction for the strategy. Of these three businesses, one explicitly mentions a desire for more reporting. Lastly, one company informs that the board is the one who determines overall policy and seems committed and supportive. Only one business in the public sector does not know what role the board has in security management.

In the private sector, two businesses inform that the board's main task is safeguarding the owners' interests. This includes ensuring that the business fulfills the duties imposed by law and regulations, that the business's values are secured, and that the business operates within an acceptable level of risk. Furthermore, another company explains that the board has an overall responsibility as set out in the board instructions, where the board owns risk appetite and criteria. It is further informed that the board participates primarily in any investments with the management. Two other businesses explain that the board is one of the policymakers for security, where they set good requirements and a good agenda for the security work in the business. Another business has a foreign owner, and the reports are therefore carried out to a foreign CISO.

5.5 What is needed to reduce the uncertainty surrounding the state of security?

Less than half of the companies examined in this survey use advanced tools to evaluate and report the state of security. Here, ServiceNow and the Governance, Risk, and Compliance (GRC) tools of their design are the regulars of the businesses that use tools. The remaining companies do not use more advanced tools other than Excel, Word, and PowerPoint. The factors influencing the businesses' use of relevant tools to evaluate and report security status are similar across all industries. When companies choose to refrain from using tools, this is due to the complexity and lack of understanding among the various available tools. This is also the biggest reason why most businesses do not use tools to assess the effects of activities and measures. Figure 5.4 shows some of the contributing factors mentioned by the companies which may lead to uncertainty.

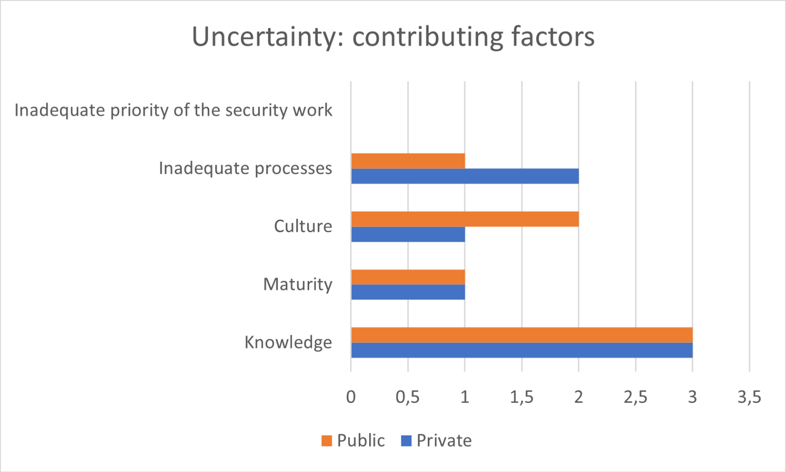

Figure 5.4: Uncertainty: Contributing factors

Four companies in the public sector explain that the company obtains information from the various operational functions to those responsible for evaluation through interviews, reports, and established services. Here, one of four businesses further explains that they have everything stored and handled in a tool where a dashboard with mandatory processes is created. Another company explains that they have a corporate goal and result management process. This process is in accordance with the “direct” process addressed in ISO 27014. Here they have something called reporting packages for tertiary reporting. The business also has a security support team that visits the companies to gather insights and develop awareness. Furthermore, another business explains that information/reporting is brought in through predefined monitoring solutions with dedicated technology, statistics from penetration testing, asset management system, and manual reports related to privacy.

In the private sector, three businesses inform that they are using the ServiceNow tool to gather information from the various operational functions to those responsible for evaluation. One of these businesses further points out a desire for greater use of indicators. Another company explains that they mainly use reports, audits, and evaluations according to frameworks. The remaining businesses inform that they do nothing other than report on sent questions to collect information from the various operational functions but that there is a desire for greater use of key performance indicators (KPIs) and benchmarking.

5.6 Is there a correspondence between the controlling authorities' experiences and what the companies answer?

The controlling authorities interviewed about their experiences of whether the various enterprises within the public and private sectors have defined security governance or management system essentially responded that very few of these have a written definition of these terms. It is experienced that it is mainly the frameworks mentioned by the businesses themselves that are commonly used, where a majority of companies use ISO 27001, and only noted that a very small number use ISO 27014. Whether the controlling authorities use the ISO 27014 framework, only one controlling authority answers that they have drawn inspiration from this. The same controlling authority also replies that they use this when they supervise. However, none of the controlling authorities use the framework themselves.

The controlling authority's experience is that the evaluation process is poorly defined in the various businesses and is not connected to the goals. Many are unaware of measuring risks, incidents, and those with more extensive audits, etc. Furthermore, they experience that the level is often set further down than in the management system. One of the controlling authorities specifies that they see that the businesses carry out security audits and controls of the company and that many do this in a good way. Nevertheless, it is experienced that they see measures that must be implemented following the management's review, but this is, to a small extent, fulfilled as they see the comprehensive measures every year.

According to the controlling authorities, it is experienced a small degree of systematic information gathering among the businesses. Only a small number of companies use tools to, among other things, evaluate and report on the state of security. ServiceNow, Remedy, and Jira are examples of such tools that the controlling authorities experience that businesses are using. Of these tools, only ServiceNow has been mentioned by the companies themselves. The remaining controlling authorities also see some use of these tools, but it can be experienced by the individual business as complex to use these and rely on more standard reporting tools such as Excel, Word, and PowerPoint.

From whom participates in the evaluation of status before management's review and who participates in management's review at the highest level, the controlling authorities experience that it is the security functions, key persons, and service owners who participate in evaluation before management's review at the businesses. They further explain that they experience that it is almost always the management team, as well as the security manager and sometimes the operations manager, who take part in the management's review. A subset of the board or a representative from the board is also perceived to participate in the management's review, but this is experienced to a somewhat lesser extent.

Chapter 6

Discussion

This chapter will discuss and align the results to each research question, describing both advantages and disadvantages. Furthermore, it elaborates on how the results relate to previous findings and the controlling authorities' experiences.

6.1 To what extent are management systems known and used?

The results from this survey and Mørketallsundersøkelsen are different. In Mørketallsundersøkelsen from 2022, it is mapped that half of the businesses that have responded have a framework or a management system for information security [23]. In this survey, all the companies either use one or more frameworks or draw inspiration from them. This difference can be justified both by the different total number of interviewees, where 2,500 businesses answered the question in Mørketallsundersøkelsen and 14 in this one, and by the fact that Mørketallsundersøkelsen has a greater range in the size and industries of the businesses interviewed.

Figure 6.1 shows companies of different sizes that use a framework or management system for information security over time. According to Mørketallsundersøkelsen, the negative development is mainly due to businesses with less than 100 employees [23]. For companies with more than 100 employees, the percentage from 2022 is at the same level as 2020. One can thus see a greater connection between the two surveys as this survey only covers companies with more than 100 employees.

According to Mørketallsundersøkelsen, there is room for interpretation for the respondents, and it is not unlikely that the definition of a framework and management system, how comprehensive it is, and how well it is implemented may vary among the respondents [23]. A decisive reason there is different information from businesses and controlling authorities on whether they have a management system may be the understanding of what it entails. Another reason is what one

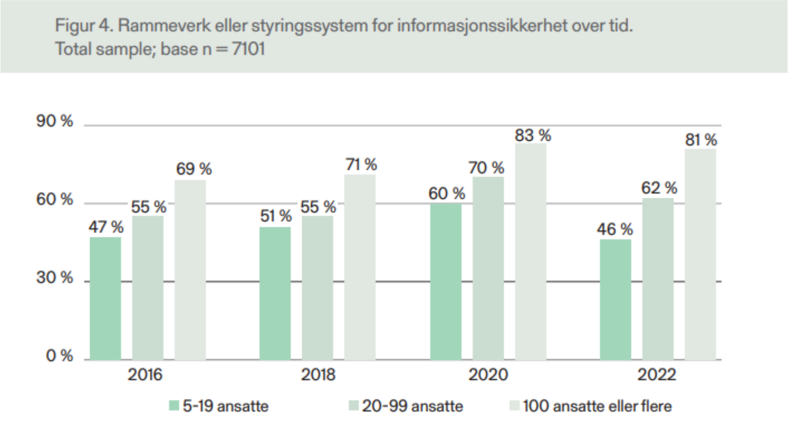

Figure 6.1: Framework or management system for information security over time. Copyright with permission by Næringslivets Sikkerhetsråd [23]

.

believes should be covered by processes, requirements, personnel, functions, tools, etc., for it to qualify for a management system. The question does not include the need for the management system should work, be measured, and be found to be sufficient to achieve reasonable security as a result. The controlling authorities are considering the latest, but the businesses have only established a goal image that they are working towards but with deficiencies of varying importance.

Most businesses have a management system, but several of these have not defined security governance according to best practices. While ISO 27001 describes requirements for management systems for information security, ISO 27014 provides a description of how the board of an enterprise should relate to such management systems for information security [2, 3]. In other words, it seems like the businesses think they follow a framework for governance when they basically only follow a framework for management systems. The same applies to the companies using the NIST CSF and PDCA cycle, which are essentially based on management systems but lack mandatory processes for the governance of information security [15].

There is a difference between having a management system and governance processes in the business. The processes included in the governance model addressed in ISO 27014 form a central basis for having governance in addition to management in the business [2]. Although most companies have a management system, they are still unfamiliar with the processes included in security governance. In many Norwegian companies, it can be noted that there is essentially a misleading understanding of the concept of security governance. Security management and security governance have different scopes and fields of application, with security work in business operations and management of security in a business. Information security management systems (ISMS) are important for controlling security in the company's operation. Still, governance is essential for this to have the necessary frames and prerequisites to function. Most of the companies in this survey use processes in the evaluation that are linked to the processes that are part of management, such as risk management and security controls etc. Therefore, many companies carry out evaluations, but not necessarily towards a common agreement on the goals set together with the board and management.

There are similar processes in ISO 27001, but ISO 27001 is more about business management. Risk management and goal achievement are central, but with the governance processes addressed in ISO 27014, one will better connect these two levels and interpret the value and opportunities for commitment and decision-making ability of the board. This may indicate that the implementation and use of both ISO 27001 and ISO 27014 are essential to ensure business outcome and stakeholders value. The use of both could help building bridges between the entities security management systems review on goal achievement and the stakeholders value from a board's perspective.

According to Mørketallsundersøkelsen, it is stated that it is worrying that only half of the Norwegian businesses have a framework or system for information security [23]. It is further revealed that those businesses that use a framework or system for information security experience somewhat more incidents than others, where most discover security breaches through internal control and security monitoring. In addition, Mørketallsundersøkelsen states that the companies who have established a management system are more robust against security incidents. It may therefore indicate that a consequence of not having a system or framework for managing information security may result in lower robustness against security incidents. It cannot, however, indicate that introducing a framework will result in businesses achieving better security than those that do not use it. This requires a more extensive mapping and data collection of cost/benefit than is available in this survey.

6.2 What is used to evaluate the state of security and to what extent is this a justified state?

The controlling authorities' experiences that the evaluation process itself is poorly defined in the various businesses and is not connected to the goals. By performing the evaluation process described in ISO 27014, the companies will be able to relate to a better data basis by assessing the business's condition against goals instead of risk management [2]. Security management requires follow-up of the company's security situation, whether correct prioritization has been carried out where there is the highest risk and not, which values are most important, and compliance with this. Implementation of this process will also be able to contribute to more effective security management by following up on the condition in a more transparent way. Finally, it will help carry out the reports at the right level, increasing the board's commitment.

A recurring theme is the degree of difficulty concerning the appraisals. This applies to both large and small businesses. Competence and culture create difficulties for the companies and the understanding of how the various values can be misused. Although the Security Act requires a careful appraisal of each business subject to this act, it is very complex and problematic for many to dive deep into their value chains and dependencies [12]. Increasing competence and providing awareness about the value chains through exercises, e-learning, conference papers, etc., are several factors that might help companies scale up their appraisals.

The fact that the businesses have carried out an appraisal is a decisive factor and a prerequisite for the company to be able to set goals, as the goals most essentially is about securing the values and the security of the company. Still, another recurring theme is the degree of difficulty for the businesses to assess whether they have achieved the various goals as they are too large and overarching. This is a central and important finding in this survey, as a lack of indicators will provide a poorer basis for evaluation and thus constitute a decisive factor. Even if the business has set goals for information security but does not have a good process for following up on these goals and assessing whether these have been achieved or is possible, the prerequisite for effective management and control will be poor. This will mainly give direction but does not contribute to the board being informed. This will primarily contribute to a certain degree of understanding by the employees in the organization of what has been set as a goal. This can, for example, be frameworks for how they work.

According to a report provided by the National Audit Office, it is explained that companies that have not compiled concrete goals and indicators base their assessment of goal achievement exclusively on descriptive qualitative goals, whether the budget balances or on carried out activities [42]. Furthermore, setting specific goals and indicators for the companies' sectoral policy tasks and efficient management can make it easier for the boards to assess and report the degree of goal achievement and efficient operation to the owner, in the opinion of the National Audit Office. They further point out that managing according to a fixed budget will give limited information about whether the management is efficient [42].

Benchmarking is also suggested as a tool to assess whether the company's operation is efficient compared to the business in the same industry [42]. This survey may indicate that several businesses are more concerned with compliance with requirements than processes. Several companies carry out risk assessments and measures based on requirements according to the frameworks and measure compliance when using these. In this way, compliance is not measured against specific security goals in the business [43].

Both the processes for non-conformity reporting and risk reporting are elements that form the data basis in the business. Suppose the firm does not have non-conformity reporting and risk reporting. In that case, the company will not have a basis for whether they are aware of non-conformities and risks that can be used in evaluating the security situation. Furthermore, this will create high uncertainty in the company as risks and deviations will be unknown. The business will not have the opportunity to defend its reporting to the board if there is insufficiency and uncertainty about which risks and deviations are present. This can result in extreme consequences if the business does not have an overview of this.

6.3 Which roles are involved in evaluating security performance?

According to NSM's basic principles for security management, the company's manager is responsible for security, where one of the manager's responsibilities is the follow-up of the preventive security work [44]. In most companies, the CEO/-manager is in charge and has delegated responsibility for information security. Still, the security management and the responsibility for the preparations for the evaluation are delegated to CISO-like roles. Many struggles with a distance in the form of an intermediary between the CEO and CISO. This distance makes it challenging to establish the need for independent GRC functions in general and security governance in particular. There is also limited communication between the board and the top management regarding the state of security in general and the performance of the management system in particular.

Figure 6.2 illustrates a governance model for an entity with one ISMS. Based on the data collection, the work is performed at the top management level, including the ISMS processes such as plan, do, check, and act. This is not at the governing body level following the governance processes, such as the evaluation process. Organizations need to work with aligned strategies at the ISMS level. Still, when asked about the evaluation process at the governing level, almost all the companies answered with what they do within the ISMS level, as the businesses do not have the processes at governing level but at the top management level. In other words, most believe that what should be done in the governing body is performed at the top management level.

The governing body is, to a minimal extent, a part of the evaluation process but, to a somehow greater extent, receives a report of the documentation of the evaluation process. However, the evaluation process mainly occurs at the top management and ISMS level, as the companies do not use the evaluation process as a governance process addressed in ISO 27014. As shown in Figure 6.2, all four governance processes create a cycle for working continuously with management and control in the business. All these processes must be followed to provide strategic direction and guidance for an enterprise's operation.

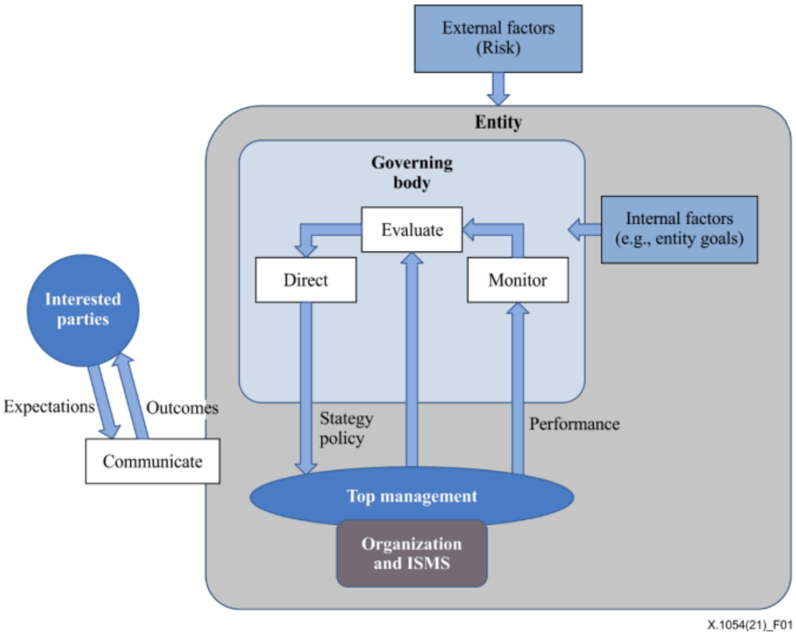

Figure 1 – Governance model for an entity with one ISMS

Figure 6.2: Governance model for an entity with one ISMS from NEK ISO/IEC 27014:2020 is reproduced by "Vilde Nylund Johnsen" in the thesis "Security governance: the board's responsibility" under licence from Standard Online AS May 2023. Standard Online makes no guarantees or warranties as to the correctness of the reproduction.

.

According to The Three Lines Model, organizations vary as to the degree of overlap and separation between the roles of the governing body and management [22]. The board is, to a minor extent, involved in the evaluation process than what they should. According to 'Styreboken´ published by PWC, a well-functioning board is characterized by having the company's real overall management, looking after its best interests and objectives, making the necessary decisions, and carrying out relevant supervision and control. Finally, it is specified that a decisive factor in safeguarding the company's interests is a good interaction between the owners and the management, where the responsibility for nurturing this relationship rests with the board [1]. In this way, the evaluation process can be a contributing factor and a key element to engage the board at a higher level.

According to NSM's basic principles for security management, the management's review is led by the company's manager, where all other managers who affect or can be affected by the security management system participate [44]. It is important to involve more than just the security management, as it will also be necessary for the business to talk to the system owners and those who own the business processes. Discussing results from those responsible for the services will be essential in the evaluation. To a small extent, it is mentioned by the companies that the business areas are involved or whether the company has conferred with them about the results concerning evaluation, reporting, and management's review. This can control the quality of the evaluation process by having the businesses, and a broadly composed group evaluate before they go to the governing body.

According to the Directorate of Digitalization, businesses should appoint a driving force in each department or at the equivalent organizational level in addition to a professional responsible for information security, depending on the size and organization of the business [43, 45, 46]. This corresponds only to a couple of the companies examined in this survey as they use security coordinators as such support. The Directorate of Digitalization further specifies that the role of promoter does not require technical ICT competence either but that the prerequisites are mainly motivation and personal suitability. This must also be assessed locally and based on the resource needs of each individual business [43, 45]. Such a role may provide a significant contribution to the company to ensure a better data basis.

According to The Three Lines Model, through all of its activities, an internal audit builds its knowledge and understanding of the organization, contributing to the assurance and advice it delivers as a trusted advisor and strategic partner [22]. From experience, the controlling authorities states that if the companies use control functions in addition to the CISO, this is essentially supported by internal and external audits, which can help to carry out controls and detect any security breaches. If the businesses use other control functions such as internal and external audits, hired consultants from consulting companies, and supervisory authorities, this will help supplement the CISO and add a better overview and control over the business. This will also be helpful if self-monitoring and evaluations are carried out in the departments/units that report to the CISO/first line. Here, some of the businesses also use compliance functions that report to the board. Furthermore, it is stated by The Three Lines Model that collaboration and communication must be across both the first- and second-line roles of management and internal audit to ensure there is no unnecessary duplication, overlap, or gaps [22].

6.4 What is needed to reduce the uncertainty surrounding the state of security?

It has been mentioned on several occasions that there is a lack of culture, competence, and maturity in the various businesses. Several companies explain that expertise in KPIs, in particular, is difficult for many as it is challenging to know what to measure and how to measure it. It is, to a minimal extent, experienced by the controlling authorities that the businesses use indicators for goal achievement. In accordance with the companies, the controlling authorities also experience a large gap in the lack of competence and understanding when using indicators for goal achievement.

This is a central and important finding in this survey as it is essential to understand that competence is necessary to be able to set good KPIs in the business and avoid these working against their purpose. KPIs can be very extensive and must be defined at all operational, tactical, and strategic levels. It is also essential that the KPIs are communicated and anchored to those for whom it is relevant, as KPIs are to help change behavior. Measuring something without doing something different based on a result is a waste of time. By increasing this competence and awareness, introducing indicators in the businesses will help strengthen security and reduce the uncertainty of each company [20, 21, 47].

The advantages of implementing both tools and security-related KPIs are the possibility of a better overview of the various business processes, seeing them in a larger context, and measuring them against each other. It will also make it easier for the business to have a better overview of the data basis and thus have better control over what is to be evaluated and what is not. If the companies do not have an overview of what they possess the effect of, they will have high uncertainty. Getting a more extensive and comprehensive overview will also help reduce uncertainty in the business. All these advantages will both improve performance and result in better governance and control at the company.

Through various audits, some of the controlling authorities have experienced that the directors of the companies do not receive enough information from the security organization. Therefore, they do not know the state of the company and are therefore not in a position to be able to answer the controlling authority's several important questions security areas. If the business has a lack of overview, the data basis of the business will be weakened. This can lead to the board and management in the industry governing incorrectly. Furthermore, this can result in unwanted events that negatively affect the business. For example, if a company within the power sector carries out management and control incorrectly, this can ultimately result in gas leaks, explosions, etc. Therefore, having a good data basis in the business is essential.

6.5 Is there a correspondence between the supervisory authorities' experiences and the companies' answers?

Where there is a correspondence between the responses from the businesses and the responses from the controlling authorities may indicate a shared understanding or agreement on how the companies operate and carry out the various processes. Nevertheless, there are several areas where there is an agreement between the businesses and the controlling authorities, but this is not necessarily positive. The fact that the companies and the controlling authorities are aware of the degree of difficulty associated with indicators of goal achievement indicates that the businesses can recognize weaknesses in the industry. Furthermore, the companies and the controlling authorities also agree on the complex and demanding area of information security rooted in each business's culture, competence, and maturity.

Where there is no correspondence between the answers from the businesses and the answers from the supervisory authorities, this may show a more remarkable variation of different understanding among the companies and the controlling authorities. This can apply to different definitions, what different processes entail, their purpose, etc. Here, there will be an opportunity for the supervisory authorities to clarify and create a new understanding among the businesses. They also have the chance to make new and targeted recommendations for the company's benefit so that knowledge is increased, and uncertainty is reduced. Different forms of organization of centralized competence environments should be considered for a closer follow-up of the companies' security governance.

It becomes clear in this survey that the supervisory authorities must ensure a more clear distinction between the terms security governance and security management. Greater emphasis should also be placed on the security management operating more closely with the business management as this could result in better and correct priorities in the various security areas. In this way, the business will be better prepared for a security incident. A rule of thumb can be to ensure that the company does the right things instead of focusing on doing various things right. The management processes in ISO 27014, especially the evaluation process, will significantly contribute to this area and minimize unnecessary work and resources [2].

One of the most significant weaknesses in security governance today is a lack of expertise and professionals. Therefore, it is essential to utilize accessibility in a social context. The governance processes, especially the evaluation process, will contribute to the business carrying out the correct priorities. If these priorities are not carried out, and we continue to act as we do to this day, there is a high probability that the threat actors will maintain and increase their lead. According to NSM in the report 'Security expert advice: A resilient Norway´, the supervisory authority confirms that a valiant effort has been carried out but that this has reduced again and that one no longer sees the effect of the various measures [8].

Chapter 7

Future work

This chapter will describe the future work of any projects in this area, including limitations encountered during this master thesis. This subject area has room for more research and analysis, and much further work can be carried out. One of the advantages of using qualitative research is the contribution to broader access to ideas and responses. Various suggestions and wishes from the different interviewees were also proposed during the interview process.

As it was desirable to create a more in-depth knowledge of the evaluation process, the methodology used in this master thesis was qualitative research. However, the advantage of using a quantitative research method would be to get a more generalized result that can describe the situation as it is [31]. This would allow the researcher to create a greater understanding of what the various findings mean, what is the actual problem, and how the companies can improve.

Early during the interview process, it was discovered that the sources available were insufficient, resulting in the companies not having the right equipment to provide a reasonable data basis to evaluate the state of security. A request that was a recurring theme for several businesses and a couple of the controlling authorities was a more adapted tool to assess and report the security condition. This would allow for a comprehensive comparison and evaluation in a greater context, which could lead to further enhancements to the system's overall performance.

Due to the limited time frame, there is some uncertainty as this survey does not have a representative sample of businesses. Although the answers given by the companies in this master thesis provide a clear indicator of the level of maturity in security governance, a greater diversity and broader range of businesses would have helped to strengthen the data basis for this task. This would allow for a comprehensive comparison and evaluation, which could further enhance the evaluation process's overall importance and performance.

During the interview process of the controlling authorities, it was early discovered the room for improvement in security governance among the companies. Based on the data collection outcomes in this study, some key elements to improve will be suggested. This would allow the controlling authorities and other stakeholders to challenge themselves to follow up on the responsibility of the board directors to a greater extent.

- The board is accountable but have limited interaction with the entity's security management.
- The board has itself to an almost non-existing degree established an independent security monitor function.
- The security performance of management systems is to a limited extent evaluated.
- There is a low-level maturity of awareness regarding the difference between security governance (board responsibility) and security management (top management) – these mutually exclusive elements of operating and controlling management systems are lacking attention.

Chapter 8

Conclusion

The first research question in this survey deals with the extent to which management systems are known and used in companies. There is a difference between having a management system and governance processes in the industry. Very few companies are familiar with the governance processes addressed in ISO 27014 and lack an understanding of how the company should relate to and measure management systems performance. As expected, almost no or very few companies have exploited this potential.

The second research question attempts to uncover what is used to evaluate the state of security and to what extent this is a justified state. All businesses answer that they either have one or more of the following elements: processes for deviation- and risk reporting and other processes and tools such as ServiceNow. These elements are measured against appraisals and goals in the company. Nevertheless, the sources available are not sufficient. As a result, several companies do not have the right equipment that provides a reasonable data basis to evaluate the state of security.

The third research question deals with which roles are involved in evaluating the security condition. Mainly, it is the top management that participates in the management review. Rarely does board members participate. Furthermore, the communication between the management and the board seems to be poor.

The fourth research question attempts to uncover what is needed to reduce the uncertainty surrounding the state of security in businesses. As expected, due to a lack of culture and competence, the companies must increase resources and knowledge to understand and interpret appropriate reporting data before the management review. Furthermore, competence is essential to ensure the correct interpretation of best practices and processes and what this entails. In this way, the companies will better understand the difference between the two frameworks, ISO 27001 and ISO 27014.

The last research question concerns whether correspondence exists between the companies and the controlling authorities answers. Here, the difference in competence and knowledge seems to be the reason for the variating correspondence between the companies and the controlling authorities. Another contributing factor may also be the different experiences of the companies and controlling authorities related to operating processes.

Many struggles with a distance in the form of an intermediary between the CEO and CISO. This distance makes it challenging to establish the need for independent GRC functions in general and security governance in particular. There is also limited communication between the board and the top management regarding the state of security in general and the performance of the management system in particular.

Based on the data collection in this study, the governing body will most likely benefit from adopting ISO 27014, particularly the evaluation process, to understand the threat picture and determine areas of governance and criteria for evaluating security performance. Furthermore, ISO 27014 will provide a great potential gain when establishing a "communication bridge" between the board and the top management. To a certain extent, this could be delivered by the evaluation process, handled by the governing body itself, or a corporate GRC function.

In this survey, it was expected uncertainty. Still, it was interesting to research the problem description presented in this master's thesis. Furthermore, it will also be interesting to see if this research work can create curiosity in others and a desire to take a closer look at ISO 27014 and what it entails. This will also create an opportunity for others to raise the strategic security work and engage the board and management to a greater extent by adopting ISO 27014 and the evaluation process.

Bibliography

[1] PWC, 'Styreboken 2023,' PWC, 2023.

[2] International Organization for Standardization, 'Information security, cybersecurity and privacy protection governance of information security,' ISO/IEC, 2020.

[3] International Organization for Standardization, 'Information technology — security techniques — information security management systems — requirements,' ISO/IEC, 2017.

[4] Årnes, Andre. 'What is the board's role in digital security?' Retrieved: 10.02.23. (2023), [Online]. Available: `https://www.linkedin.com/feed/update/urn:li:activity:7028663653184778240/`.

[5] A. D. V. PhD and J. H. P. E. PhD, 'An information security governance framework,' *Information Systems Management*, vol. 24, no. 4, pp. 361–372, 2007. DOI: `10.1080/10580530701586136`. eprint: `https://doi.org/10.1080/10580530701586136`. [Online]. Available: `https://doi.org/10.1080/10580530701586136`.

[6] B. et al., 'Proposed practices to mitigate significant mobility security risks,' *Economics Research Journal*, vol. 14, no. 1, p. 22, 2015.

[7] A. A. Al Batayneh, M. Qasaimeh and R. S. Al-Qassas, 'A scoring system for information security governance framework using deep learning algorithms: A case study on the banking sector,' *J. Data and Information Quality*, vol. 13, no. 2, Jun. 2021, ISSN: 1936-1955. DOI: `10.1145/3418172`. [Online]. Available: `https://doi.org/10.1145/3418172`.

[8] NSM, 'Sikkerhetsfaglig råd 2023: Et motstandsyktig norge,' NSM, 2023.

[9] T. E. PARLIAMENT and T. COUNCIL, 'Sthe nis2 (network and information systems) directive 2,' European parlament, 2023.

[10] Schjetne, Steinar. 'Kripos mener å ha oppklart løsepenge-angrepet mot hydro.' Retrieved: 26.05.2023. (Apr. 2023), [Online]. Available: `https://e24.no/naeringsliv/i/EQ5m6K/kripos-mener-aa-ha-oppklart-loesepenge-angrepet-mot-hydro`.

[11] Lysberg, Magnus. Stolt-Nielsen, Harald. 'Dataangrepet kostet hydro 800 millioner kroner. nå er det kriminelle nettverket avdekket.' Retrieved: 24.04.2023. (Nov. 2022), [Online]. Available: `https://www.aftenposten.no/norge/i/47WR3o/dataangrepet-kostet-hydro-800-millioner-kroner-naa-er-det-kriminelle-nettverket-avdekket`.

[12] Lovdata. 'Lov om nasjonal sikkerhet (sikkerhetsloven).' Retrieved: 14.03.23. (2023), [Online]. Available: `https://lovdata.no/dokument/NL/lov/2018-06-01-24`.

[13] Lovdata. 'Forskrift om virksomheters arbeid med forebyggende sikkerhet (virksomhetsikkerhetsforskriften).' Retrieved: 14.03.23. (2023), [Online]. Available: `https://lovdata.no/dokument/SF/forskrift/2018-12-20-2053`.

[14] T. N. I. of Standards and Technology, 'The nist cybersecurity framework,' NIST, 2018.

[15] IT Governance. 'Nist cybersecurity framework (csf).' Retrieved: 14.03.23. (2023), [Online]. Available: `https://www.itgovernance.co.uk/nist-cybersecurity-framework`.

[16] AXELOS. 'What is itil?' Retrieved: 14.02.23. (2023), [Online]. Available: `https://www.axelos.com/certifications/itil-service-management/what-is-itil`.

[17] AXELOS, 'Itil foundation, 4th edition,' The Stationary Office (TSO), 2019.

[18] N. Standard, 'Requirements for risk assessment,' Norsk Standard, 2021.

[19] Nasjonal Sikkerhetsmyndighet. 'Grunnprinsipper for ikt-sikkerhet.' Retrieved: 03.11.22. (Nov. 2022), [Online]. Available: `https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/grunnprinsipper-ikt`.

[20] A. Jaquith, *Security Metrics: Replacing Fear, Uncertainty, and Doubt*. London: Pearson Education, 2007.

[21] C. O. for Business Information-related Technology, 'Cobit framework,' COBIT, 2019.

[22] T. I. of Internal Auditors, 'The iia's three lines model,' IIA, 2020.

[23] N. sikkerhetsråd, 'Mørketallsundersøkelsen 2022,' Næringslivets sikkerhetsråd, 2022.

[24] R. Manchke, 'The applicability of iso 27014:2013 for use within general medical practice,' Edith Cowan University, 2013.

[25] T. A. Zia, 'Organisations capability and aptitude towards it security governance,' in *2015 5th International Conference on IT Convergence and Security (ICITCS)*, 2015, pp. 1–4. DOI: `10.1109/ICITCS.2015.7293005`.

[26] Maynard, Sean B. Tan, Terrence. Ahmad, Atif. Ruighave, Tobias. 'Towards a framework for strategic security context in information security governance.' Retrieved: 11.11.22. (Nov. 2022), [Online]. Available: `https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1185%5C&context=pajais`.

[27] R. von Solms and S. (Basie) von Solms, 'Information security governance: A model based on the direct–control cycle,' *Computers & Security*, vol. 25, no. 6, pp. 408–412, 2006, ISSN: 0167-4048. DOI: `https://doi.org/10.1016/j.cose.2006.07.005`. [Online]. Available: `https://www.sciencedirect.com/science/article/pii/S0167404806001167`.

[28] A. et al., 'Information security governance: A process model and pilot case study,' *Short paper*, vol. 10, no. 3, p. 10, 2020.

[29] T. Salmenpää, 'Information security governance in civil aviation,' in *Cyber Security: Critical Infrastructure Protection*, M. Lehto and P. Neittaanmäki, Eds. Cham: Springer International Publishing, 2022, pp. 315–336, ISBN: 978-3-030-91293-2. DOI: `10.1007/978-3-030-91293-2_13`. [Online]. Available: `https://doi.org/10.1007/978-3-030-91293-2_13`.

[30] C.-C. Huang, K.-J. Farn and F. Y.-S. Lin, 'A study on isms policy: Importing personal data protection of isms,' *Journal of Computers*, vol. 23, no. 1, pp. 35–41, 2012.

[31] J. E. Leedy Paul D. Ormrod, *Practical Research: Planning and Design*. London: Pearson, 2016.

[32] A. Tjora, *Kvalitative forskningsmetoder i praksis*. Oslo: Gyldendal, 2021.

[33] L. Wong, 'Data analysis in qualitative research: A brief guide to using nvivo,' National Library of Medicin, 2008.

[34] K. L. Vik. 'Nvivo.' Retrieved: 13.05.21. (Aug. 2020), [Online]. Available: `https://innsida.ntnu.no/wiki/-/wiki/Norsk/NVivo`.

[35] NVIVO. 'Data security and privacy.' Retrieved: 06.04.21. (), [Online]. Available: `https://help.mynvivo.com/nvtranscription/Content/NVT_data_security.htm`.

[36] A. H. Alabri Saleh Said. Hilal, 'Using nvivo for data analysis in qualitative reserach,' Ministry of education, Sultanate of Oman, 2013.

[37] NYU. 'Qualitative data analysis.' Retrieved: 20.03.2023. (), [Online]. Available: `https://guides.nyu.edu/QDA/atlasti`.

[38] M. e. a. Peters, 'Guidance for conducting systematic scoping reviews,' Sep. 2015.

[39] M. Byrne, E. Keary and A. Lawton, 'How to conduct a literature review,' Aug. 2012.

[40] L. Arskey Hilary. O'Malley, 'Scoping studies: Towards a methodological framework,' Feb. 2007.

[41] NHO. 'Fakta om små og mellomstore bedrifter (smb).' Retrieved: 20.03.2023. (), [Online]. Available: `https://www.nho.no/tema/sma-og-mellomstore-bedrifter/artikler/sma-og-mellomstore-bedrifter-smb/`.

[42] Riksrevisjonen, 'Mål og indikatorer for måloppnåelse og effektiv drift i heleide selskaper der staten har en samfunnsmessig begrunnelse eller et sektorpolitisk mål med eierskapet,' Riksrevisjonen, 2018.

[43] Digitaliseringsdirektoratet. 'Fellestrekk for styring og kontroll.' Retrieved: 24.04.23. (2023), [Online]. Available: `https://www.digdir.no/informasjonssikkerhet/fellestrekk-styring-og-kontroll/2278`.

[44] Nasjonal Sikkerhetsmyndighet. 'Grunnprinsipper for sikkerhetsstyring.' Retrieved: 03.04.23. (2023), [Online]. Available: `https://nsm.no/getfile.php/134493-1605693992/NSM/Filer/Dokumenter/Grunnprinsipper%5C%20for%5C%20sikkerhetsstyring.pdf`.

[45] Digitaliseringsdirektoratet. 'Suksesskriterier for styring av informasjonssikkerhet.' Retrieved: 24.04.23. (2023), [Online]. Available: `https://www.digdir.no/informasjonssikkerhet/suksesskriterier-styring-av-informasjonssikkerhet/3146`.

[46] Digitaliseringsdirektoratet. 'Ulike perspektiver gir ulikt fokus.' Retrieved: 24.04.23. (2023), [Online]. Available: `https://www.digdir.no/informasjonssikkerhet/ulike-perspektiver-gir-ulikt-fokus/2279`.

[47] Sorteberg, Hanne Rygg. 'Hva er en god kpi – og hvordan unngå at de virker mot sin hensikt?' Retrieved: 10.05.23. (2023), [Online]. Available: `https://www.linkedin.com/pulse/hva-er-en-god-kpi-og-hvordan-unng%5C%C3%5C%A5-de-virker-mot-sin-sorteberg/?originalSubdomain=no`.

Appendix A

Data processing form

The data processing form that was sent out to all interviewees for signature prior to the interview.

Med dette dokumentet bekrefter jeg, Vilde Nylund Johnsen at all innsamling av data til masteroppgaven "Sikkerhet i styrerommet" vil holdes internt, og når data er ferdigbehandlet vil det slettes. Innleveringsfristen for masteroppgaven er den 1. Juni, og databehandlingen vil ansees som ferdig innen da.

Svar på intervjuspørsmålene trekkes inn i analysen, men transkripsjon av intervjuet vil ikke publiseres i eller utenfor oppgaven.

I det tilfellet at intervjuobjektet ønsker å være anonyme vil fremdeles størrelse på bedriften og sektor bedriften tilhører beskrives, men all annen informasjon vil anonymiseres.

Det ønskes at bedriften selv, i dette dokumentet velger om de ønsker å være anonym eller ei, og anerkjenner at dokumentet er lest og godkjent.

Jeg bekrefter at vår bedrift ønsker å være anonym [ ]
Jeg bekrefter at vår bedrift ikke ønsker å være anonym [ ]

Jeg bekrefter at dokumentet er lest og godkjent [ ]

Dato: ________________

Bedrift: ____________________

Representant for bedrift: _________________

Signatur: __________________

Dato: _07.02.2023_____________

Vilde Nylund Johnsen: ______Vilde Nylund________________________

Appendix B

Interview guide - companies

The complete interview guide with all questions, theory and purpose.

Kategori 1: Rammebetingelser og krav – kategori for å understøtte etterlevelse – ta inn kontekst her

1.1	**Teori**: Sikkerhetsstyring: «The definition of governance of information security is the means by which an organization's governing body provides overall direction and control of activities that affect the security of an organization's information» ISO27014 **Spørsmål**: Har bedriften en gitt definisjon av sikkerhetsstyring? **Hensikt**: Hensikten med spørsmålet er å kartlegge de ulike definisjonene som benyttes og avgjøre om det er en felles enighet om hva sikkerhetsstyring er og innebærer. Svar:

1.2	**Teori**: Styringssystem: «The organization shall establish, implement, maintain and continually improve an information security management system, including the processes needed and their interactions, in accordance with the requirements of this document. » ISO27001 **Spørsmål**: Har bedriften en gitt definisjon av styringssystem? **Hensikt**: Hensikten med spørsmålet er å kartlegge de ulike definisjonene som benyttes og avgjøre om det er en felles enighet om hva et styringssystem er og innebærer. Svar:

1.3	**Teori**: Se sikkerhetsloven, kap 4 § 4-1: sikkerhetsstyring. Virksomhetens leder har ansvar for det forebyggende sikkerhetsarbeidet. Se også sikkerhetsloven, kap 4 § 4-4: krav til dokumentasjon. Virksomheten skal dokumentere vurderingen av risiko og de gjennomførte og planlagte sikkerhetstiltakene. 7 av 10 bedrifter har et rammeverk og/eller et styringssystem for informasjonssikkerhet (se mørketallsrapporten). Rapportering til datatilsynet → se personopplysningssikkerhetsloven, artikkel 33: Melding til tilsynsmyndigheten om brudd på personopplysningssikkerheten. Ved brudd på personopplysningssikkerheten skal den behandlingsansvarlige uten ugrunnet opphold og når det er mulig, senest 72 timer etter å ha fått kjennskap til det, melde bruddet til vedkommende tilsynsmyndighet i samsvar med artikkel 55, med mindre bruddet sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter. Dersom bruddet ikke meldes til tilsynsmyndigheten innen 72 timer, skal årsakene til forsinkelsen oppgis. **Spørsmål**: Har bedriften/organisasjonen et system eller et rammeverk for styring av informasjonssikkerhet? **Hensikt**: Hensikten med spørsmålet er å se om bruk av et system eller et rammeverk for styring har noe å si for hvordan bedriften styrer, blant annet se på om de som benytter seg av et system/rammeverk gjennomfører styring i bedriften på en mer effektiv måte. Svar:

1.4	**Teori**: ISO27014/ISO27001 **Spørsmål**: Benytter bedriften seg av rammeverket ISO27014 og/eller ISO27001? Hvordan bruker dere i så fall rammeverket? Helt eller delvis? **Hensikt**: Hensikten med spørsmålet er å kartlegge om bedriften benytter seg av et spesifikt rammeverk i arbeidet med sikkerhetsstyring og kommunikasjon med styret. Svar:

1.4.1	**Teori**: Hvis nei på forrige **Spørsmål**: Dersom bedriften ikke benytter seg av ISO27014 og/eller ISO27001 eller andre relevante rammeverk, hvilke vurderinger ligger til grunn for valget? **Hensikt**: Hensikten med spørsmålet er å kartlegge om hvordan bedriften vurderer verdien av å bruke beste praksis som grunnlag for dialogen med styret. Svar:

1.5	**Teori**: ISO 27014 **Spørsmål**: Er bedriften kjent med prosessene «monitor», «direct», «communicate», and «evaluate» som inngår i styringsprosessen og/eller benytter seg av andre definerte prosesser for styring? **Hensikt**: Hensikten med spørsmålet er å undersøke i hvilken grad bedriften jobber prosessorientert med sikkerhetsstyring. Svar:

1.6	**Teori**: Se sikkerhetsloven, GDPR, kraftberedskapsforskriften etc. **Spørsmål**: Hvilke lover og regler er bedriften underlagt og setter noen av disse regelverkene krav til evalueringsprosessen og styrets ansvar for sikkerhet? **Hensikt**: Hensikten med spørsmålet er å kartlegge lovpålagte krav til evaluering og styrets ansvar for sikkerhet. Svar:

1.7	**Teori**: Se sikkerhetsloven, GDPR, kraftberedskapssforskriften etc. **Spørsmål**: Benytter bedriften seg av sektor spesifikke regler eller normer for evalueringsprosessen og styringssystem? **Hensikt**: Hensikten med spørsmålet er å kartlegge ulike reguleringer i ulike bransjer og sektorer og hvordan dette påvirker styrets involvering. Svar:

Kategori 2: Verdier og mål

2.1	**Teori**: ISO 27014 / ISO 27001 / NIST / Nasjonal sikkerhetslov. Lovpålagte krav og beste praksis for å kartlegge, vurdere og ivareta nasjonale sikkerhetsinteresser, samfunnsfunksjoner og andre interesser og verdier i ulike bransjer og sektorer. **Spørsmål**: Har bedriften en oversikt over verdiene i bedriften og deres respektive kritikalitet? **Hensikt**: Hensikten med spørsmålet er å undersøke i hvilken grad bedriften evaluerer sikkerhet mot bedriften sine verdier og/eller mål. Svar:

2.2	**Teori**: ISO 27014 / ISO 27001 **Spørsmål**: Hvor/hvordan blir verdiene fastsatt i bedriften? **Hensikt**: Hensikten med spørsmålet er å undersøke om beslutningsprosessen påvirker evalueringsprosessen og styrets involvering i sikkerhetsstyringen. Svar:

2.3	**Teori**: ISO 27014 / ISO 27001. Se sikkerhetsloven. **Spørsmål**: Har bedriften noen satte mål for informasjonssikkerhet? Hvilke prosesser benyttes for fastsettelse, og hvor besluttes dette? **Hensikt**: Hensikten med spørsmålet er å se på hva som ligger til grunn for evaluering av sikkerhetstilstand. Svar:

2.4	**Teori**: ISO 27014 / ISO 27001 / NIST CSF. Se sikkerhetsloven.

	Spørsmål: Hvordan avgjør bedriften om de satte målene er oppnådd og/eller mulige? **Hensikt**: Hensikten med spørsmålet er å vurdere grunnlaget for styrets engasjement og evne/forutsetninger for å styre – hvor viktig er evalueringsprosessen? Svar:

Kategori 3: Organisering – hvem gjør hva og hvordan gjør de det

3.1	**Teori**: ISO27014 **Spørsmål**: Hvordan jobber bedriften med evalueringsprosessen og hva inngår i denne prosessen? **Hensikt**: Hensikten med spørsmålet er å undersøke hvordan bedriften jobber med grunnlaget for ledelsens gjennomgang. Svar:

3.2	**Teori**: ISO 27014 / NSMs Grunnprinsipper for sikkerhetsstyring **Spørsmål**: Hva er grunnlaget for ledelsens gjennomgang? **Hensikt**: Hensikten med spørsmålet er å undersøke hvordan bedriften jobber med grunnlaget for ledelsens gjennomgang. Svar:

3.3	**Teori**: ISO 27014 / ISO 27001 / NSMs Grunnprinsipper for sikkerhetsstyring **Spørsmål**: Hvordan har bedriften organisert ansvar for informasjonssikkerhet? **Hensikt**: Hensikten med spørsmålet er å kartlegge utslag av plassering av sikkerhetsansvar på styrets engasjement. Svar:

3.4	**Teori**: ISO 27014 / PWC styreboken **Spørsmål**: Hvem gir oppdrag til CISO/CSO (eller tilsvarende)? **Hensikt**: Hensikten med spørsmålet er å undersøke om plassering av CISO og oppdragsansvar

	påvirker effekten av evalueringsprosessen og styrets interesse og involvering. Svar:

3.5	**Teori**: ISO 27014 **Spørsmål**: Hvor/i hvilken rolle har bedriften plassert ansvar for evaluering av sikkerhetstilstand og måloppnåelse? **Hensikt**: Hensikten med spørsmålet er å identifisere utslag av plassering av evalueringsansvaret. Svar:

3.6	**Teori**: ISO 27014 / ISO 27001 **Spørsmål**: Benytter bedriften seg av andre kontrollfunksjoner enn CISO for å følge opp status og grunnlag for evaluering? **Hensikt**: Hensikten med spørsmålet er å identifisere effekten av organiseringen og plassering av kontrollfunksjoner. Svar:

3.7	**Teori**: ISO 27014 **Spørsmål**: Hvordan henter bedriften informasjon/rapportering fra de ulike operative funksjonene til ansvarlig for evaluering? **Hensikt**: Hensikten med spørsmålet er å identifisere utslag av rapporteringsprosesser. Svar:

Kategori 4: Evalueringsprosessen – om måla er oppnådd eller mulige

4.1	**Teori**: Se sikkerhetsloven **Spørsmål**: Har bedriften definert indikatorer for måloppnåelse? **Hensikt:** Hensikten med spørsmålet er å undersøke hva som danner grunnlaget for evalueringen. Svar:

4.2	**Teori**: ISO 27014 **Spørsmål**: Benytter bedriften noen form for verktøy for å sikre datagrunnlag og vurdere effekter av aktiviteter og tiltak (herunder investeringer i sikkerhet)? **Hensikt**: Hensikten med spørsmålet er å undersøke om tilgang til aktuelle verktøy for evaluering og rapportering og om bedrifter tar i bruk KPIs, OKR, etc. Svar:

4.3	**Teori**: ISO 27014 **Spørsmål**: Mener bedriften at det er god tilgang til relevante verktøy for å evaluere og rapportere sikkerhetstilstand? **Hensikt**: Hensikten med spørsmålet er å undersøke om tilgang til aktuelle verktøy for evaluering og rapportering. Svar:

4.4	**Teori**: Se sikkerhetsloven **Spørsmål**: Har bedriften en prosess for avviksrapportering som inngår i grunnlaget for evaluering av sikkerhetstilstand? **Hensikt**: Hensikten med spørsmålet er å undersøke om bedriften har en prosess for avviksrapportering som inngår i evalueringsprosessen. Svar:

4.5	**Teori**: Se sikkerhetsloven **Spørsmål**: Har bedriften en prosess for risikorapportering som inngår i grunnlaget for evaluering av sikkerhetstilstand? **Hensikt**: Hensikten med spørsmålet er å undersøke om bedriften har en prosess for risikorapportering som inngår i evalueringsprosessen. Svar:

4.6	**Teori**: ISO27014 **Spørsmål**: Har bedriften satt krav til hvilke evalueringer som skal gjøres i ulike deler av organisasjonen? (hva skal evalueres)

	Hensikt: Hensikten med spørsmålet er å undersøke hvordan bedriften innhenter datagrunnlag for evaluering. Svar:

4.7	**Teori**: ISO27014 **Spørsmål**: Hvem i bedriften deltar i evaluering av status før ledelsens gjennomgang? Og hvem deltar i ledelsens gjennomgang på øverste nivå? **Hensikt:** Hensikten med spørsmålet er å undersøke hvilke interessenter som er direkte involvert i underlaget for dialogen med styret. Svar:

4.8	**Teori**: ISO27014 **Spørsmål**: Hvor ofte gjennomfører bedriften evaluering? **Hensikt:** Hensikten med spørsmålet er å undersøke hvordan bedriften jobber med evalueringsprosessen. Svar:

4.9	**Teori**: ISO27014 **Spørsmål**: Hvordan dokumenterer bedriften evalueringsprosessen? **Hensikt:** Hensikten med spørsmålet er å undersøke hvordan bedriften jobber med evalueringsprosessen. Svar:

4.10	**Teori**: ISO27014 **Spørsmål**: Hvem i bedriften blir orientert om resultatet av evalueringsprosessen/årlig evaluering? **Hensikt:** Hensikten med spørsmålet er å avdekke ulike ansvarsområder i bedriften når det gjelder evalueringsprosessen. Svar:

Kategori 5: Forholdet til styret

5.1	**Teori**: ISO 27014 **Spørsmål**: Hvem i bedriften er ansvarlig for informasjon og dialog med styret om sikkerhetstilstanden? Hvilken eventuell rolle har CSO/CISO i dialogen? **Hensikt**: Hensikten med spørsmålet er å kartlegge og avdekke ulike ansvarsområder mellom styret og sikkerhetsledelsen. Svar:

5.2	**Teori**: ISO 27014 / PWC styreboken **Spørsmål**: Hvilken rolle har styret i sikkerhetsstyringen? **Hensikt**: Hensikten med spørsmålet er å undersøke om i hvilken grad styret engasjerer seg aktivt i fastsettelse av retning og evaluering av effekter av investeringer og tiltak. svar:

5.3	**Teori**: ISO 27014 **Spørsmål**: Hvordan følges evalueringsprosessen opp med styret? **Hensikt**: Hensikten med spørsmålet er å undersøke ulike prosesser og løsninger for å sikre styrets involvering, interesse og forståelse for sin rolle knyttet til sikkerhetsstyring. Svar:

Appendix C

Interview guide - controlling authorities

The complete interview guide with all questions, theory and purpose.

Kategori 1: Rammebetingelser og krav – kategori for å understøtte etterlevelse – ta inn kontekst her

1.1 **Teori**: Sikkerhetsstyring: «The definition of governance of information security is the means by which an organization's governing body provides overall direction and control of activities that affect the security of an organization's information» ISO 27014

Spørsmål: Har dere erfaring som tilsynsmyndighet at ulike bedrifter har definert sikkerhetsstyring?

Hensikt: Hensikten med spørsmålet er å kartlegge de ulike definisjonene som benyttes og avgjøre om det er en felles enighet om hva sikkerhetsstyring er og innebærer.

Svar:

1.2 **Teori**: Styringssystem: «The organization shall establish, implement, maintain and continually improve an information security management system, including the processes needed and their interactions, in accordance with the requirements of this document. » ISO27001

Spørsmål: Har dere erfaring som tilsynsmyndighet at ulike bedrifter har definert et styringssystem?

Hensikt: Hensikten med spørsmålet er å kartlegge de ulike definisjonene som benyttes og avgjøre om det er en felles enighet om hva et styringssystem er og innebærer.

Svar:

1.3 **Teori**: Se sikkerhetsloven, kap 4 § 4-1: sikkerhetsstyring. Virksomhetens leder har ansvar for det forebyggende sikkerhetsarbeidet. Se også sikkerhetsloven, kap 4 § 4-4: krav til dokumentasjon. Virksomheten skal dokumentere vurderingen av risiko og de gjennomførte og planlagte sikkerhetstiltakene. 7 av 10 bedrifter har et rammeverk og/eller et styringssystem for informasjonssikkerhet (se mørketallsrapporten). Rapportering til datatilsynet → se personopplysningssikkerhetsloven, artikkel 33: Melding til tilsynsmyndigheten om brudd på personopplysningssikkerheten. Ved brudd på personopplysningssikkerheten skal den behandlingsansvarlige uten ugrunnet opphold og når det er mulig, senest 72 timer etter å ha fått kjennskap til det, melde bruddet til vedkommende tilsynsmyndighet i samsvar med artikkel 55, med mindre bruddet sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter. Dersom bruddet ikke meldes til tilsynsmyndigheten innen 72 timer, skal årsakene til forsinkelsen oppgis.

Spørsmål: Har dere erfaring som tilsynsmyndighet at ulike bedrifter/organisasjoner benytter seg av et system eller et rammeverk for styring av informasjonssikkerhet?

Hensikt: Hensikten med spørsmålet er å se om bruk av et system eller et rammeverk for styring har noe å si for hvordan bedriften styrer, blant annet se på om de som benytter seg av et system/rammeverk gjennomfører styring i bedriften på en mer effektiv måte.

	Svar:

1.4	**Teori**: ISO27014/ISO2701 **Spørsmål**: Har dere erfaring som tilsynsmyndighet at ulike bedrifter benytter seg av rammeverket ISO27014 og/eller ISO27001? Har dere videre erfaring med hvordan de bruker det? Helt eller delvis? **Hensikt**: Hensikten med spørsmålet er å kartlegge om bedriften benytter seg av et spesifikt rammeverk i arbeidet med sikkerhetsstyring og kommunikasjon med styret. Svar:

1.4.1	**Teori**: Hvis nei på forrige **Spørsmål**: Dersom bedriften ikke benytter seg av ISO27014 og/eller ISO2701 eller andre relevante rammeverk, har dere erfaring som tilsynsmyndighet om hvilke vurderinger som ligger til grunn for valget hos bedriften? **Hensikt**: Hensikten med spørsmålet er å kartlegge om hvordan bedriften vurderer verdien av å bruke beste praksis som grunnlag for dialogen med styret. Svar:

1.5	**Teori**: ISO 27014 **Spørsmål**: Har dere som tilsynsmyndighet erfaring om bedriften er kjent med prosessene «monitor», «direct», «communicate», and «evaluate» som inngår i styringsprosessen og/eller benytter seg av andre definerte prosesser for styring? **Hensikt**: Hensikten med spørsmålet er å undersøke i hvilken grad bedriften jobber prosessorientert med sikkerhetsstyring. Svar:

1.6	**Teori**: ISO 27014 **Spørsmål**: I hvilken grad bruker dere som tilsynsmyndighet rammeverket ISO 27014? **Hensikt**: Hensikten med spørsmålet er å kartlegge om tilsynsmyndighetene selv benytter seg av rammeverket ISO 27014 og om dette utgjør en relevans/forskjell. Svar:

1.7	**Teori**: ISO 27014 **Spørsmål**: Måler dere som tilsynsmyndighet opp mot ISO 27014? **Hensikt**: Hensikten med spørsmålet er å kartlegge om tilsynsmyndighetene selv benytter seg av rammeverket ISO 27014 og om dette utgjør en relevans/forskjell. Svar:

1.8	**Teori**: Se sikkerhetsloven, GDPR, kraftberedskapsforskriften etc. **Spørsmål**: Har dere som tilsynsmyndighet erfaring med hvilke lover og regler bedriften er underlagt og om noen av disse regelverkene setter krav til evalueringsprosessen og styrets ansvar for sikkerhet? **Hensikt**: Hensikten med spørsmålet er å kartlegge lovpålagte krav til evaluering og styrets ansvar for sikkerhet. Svar:

1.9	**Teori**: Se sikkerhetsloven, GDPR, kraftberedskapsforskriften etc. **Spørsmål**: Har dere som tilsynsmyndighet erfaring om bedriften benytter seg av sektor spesifikke regler eller normer for evalueringsprosessen og styringssystem? **Hensikt**: Hensikten med spørsmålet er å kartlegge ulike reguleringer i ulike bransjer og sektorer og hvordan dette påvirker styrets involvering. Svar:

Kategori 2: Verdier og mål

2.1	**Teori**: ISO 27014 / ISO 27001 / NIST / Nasjonal sikkerhetslov. Lovpålagte krav og beste praksis for å kartlegge, vurdere og ivareta nasjonale sikkerhetsinteresser, samfunnsfunksjoner og andre interesser og verdier i ulike bransjer og sektorer. **Spørsmål**: Har dere som tilsynsmyndighet erfaring om de ulike bedriftene har en oversikt over verdiene i bedriften og deres respektive kritikalitet? **Hensikt**: Hensikten med spørsmålet er å undersøke i hvilken grad bedriften evaluerer sikkerhet mot bedriften sine verdier og/eller mål. Svar:

2.2	**Teori**: ISO 27014 / ISO 27001 **Spørsmål**: Har dere som tilsynsmyndighet erfaring om hvor/hvordan verdiene blir fastsatt i bedriften? **Hensikt**: Hensikten med spørsmålet er å undersøke om beslutningsprosessen påvirker evalueringsprosessen og styrets involvering i sikkerhetsstyringen. Svar:

2.3	**Teori**: ISO 27014 / ISO 27001. Se sikkerhetsloven. **Spørsmål**: Har dere som tilsynsmyndighet erfaring om de ulike bedriftene har noen satte mål for informasjonssikkerhet? Hvilke prosesser benyttes for fastsettelse og hvor besluttes dette? **Hensikt**: Hensikten med spørsmålet er å se på hva som ligger til grunn for evaluering av sikkerhetstilstand. Svar:

2.4	**Teori**: ISO 27014 / NIST CSF. Se sikkerhetsloven. **Spørsmål**: Har dere som tilsynsmyndighet erfaring om hvordan de ulike bedriftene avgjør om de satte målene er oppnådd og/eller mulige? **Hensikt**: Hensikten med spørsmålet er å vurdere grunnlaget for styrets engasjement og evne/forutsetninger for å styre – hvor viktig er evalueringsprosessen? Svar:

Kategori 3: Organisering – hvem gjør hva og hvordan gjør de det

3.1	**Teori**: ISO27014 **Spørsmål**: Har dere som tilsynsmyndighet erfaring om hvordan ulike bedrifter jobber med evalueringsprosessen og hva som inngår i denne prosessen? **Hensikt**: Hensikten med spørsmålet er å undersøke hvordan bedriften jobber med grunnlaget for ledelsens gjennomgang. Svar:

3.2	**Teori**: ISO 27014 / NSMs Grunnprinsipper for sikkerhetsstyring **Spørsmål**: Har dere som tilsynsmyndighet erfaring om hva grunnlaget er for ledelsens gjennomgang? **Hensikt**: Hensikten med spørsmålet er å undersøke hvordan bedriften jobber med grunnlaget for ledelsens gjennomgang. Svar:

3.3	**Teori**: ISO 27014 / ISO 27001 / NSMs Grunnprinsipper for sikkerhetsstyring **Spørsmål**: Har dere som tilsynsmyndighet erfaring om hvordan de ulike bedriftene har organisert ansvar for informasjonssikkerhet? **Hensikt**: Hensikten med spørsmålet er å kartlegge utslag av plassering av sikkerhetsansvar på styrets engasjement. Svar:

3.4	**Teori**: ISO 27014 / PWC styreboken **Spørsmål**: Har dere som tilsynsmyndighet erfaring om hvem som gir oppdrag til CISO/CSO (eller tilsvarende)? **Hensikt**: Hensikten med spørsmålet er å undersøke om plassering av CISO og oppdragsansvar påvirker effekten av evalueringsprosessen og styrets interesse og involvering. Svar:

3.5	**Teori**: ISO 27014 / ISO 27001 **Spørsmål**: Har dere som tilsynsmyndighet erfaring om hvor/i hvilken rolle bedriften har plassert ansvar for evaluering av sikkerhetstilstand og måloppnåelse? **Hensikt**: Hensikten med spørsmålet er å identifisere utslag av plassering av evalueringsansvaret. Svar:

3.6	**Teori**: ISO 27014 / ISO 27001 **Spørsmål**: Har dere som tilsynsmyndighet erfaring om ulike bedrifter benytter seg av andre kontrollfunksjoner enn CISO for å følge opp status og grunnlag for evaluering? **Hensikt**: Hensikten med spørsmålet er å identifisere effekten av organiseringen og plassering av

	kontrollfunksjoner. Svar:

3.7	**Teori**: ISO 27014 **Spørsmål**: Har dere som tilsynsmyndighet erfaring om hvordan bedriften henter informasjon/rapportering fra de ulike operative funksjonene til ansvarlig for evaluering? **Hensikt**: Hensikten med spørsmålet er å identifisere utslag av rapporteringsprosesser. Svar:

3.8	**Teori**: ISO 27014 / andre kilder **Spørsmål**: Hvilke kilder bruker dere som tilsynsmyndighet for å få inn rapportering, f.eks. avvikssystem, risikorapportering, compliance rapportering etc.? **Hensikt**: Hensikten med spørsmålet er å identifisere og kartlegge hvilke kilder tilsynsmyndigheten tar i bruk for å få inn rapportering. Svar:

Kategori 4: Evalueringsprosessen – om måla er oppnådd eller mulige

4.1	**Teori**: Se sikkerhetsloven **Spørsmål**: Har dere som tilsynsmyndighet erfaring om ulike bedrifter har definert indikatorer for måloppnåelse? **Hensikt:** Hensikten med spørsmålet er å undersøke hva som danner grunnlaget for evalueringen. Svar:

4.2	**Teori**: ISO 27014 **Spørsmål**: Har dere som tilsynsmyndighet erfaring om de ulike bedriftene benytter noen form for verktøy for å sikre datagrunnlag og vurdere effekter av aktiviteter og tiltak (herunder investeringer i sikkerhet)? **Hensikt**: Hensikten med spørsmålet er å undersøke om tilgang til aktuelle verktøy for evaluering og rapportering og om bedrifter tar i bruk KPIs, OKR, etc.

	Svar:

4.3	**Teori**: ISO 27014 **Spørsmål**: Har dere som tilsynsmyndighet erfaring om de ulike bedriftene mener at det er god tilgang til relevante verktøy for å evaluere og rapportere sikkerhetstilstand? **Hensikt**: Hensikten med spørsmålet er å undersøke om tilgang til aktuelle verktøy for evaluering og rapportering. Svar:

4.4	**Teori**: Se sikkerhetsloven **Spørsmål**: Har dere som tilsynsmyndighet erfaring om bedriften har en prosess for avviksrapportering som inngår i grunnlaget for evaluering av sikkerhetstilstand? **Hensikt**: Hensikten med spørsmålet er å undersøke om bedriften har en prosess for avviksrapportering som inngår i evalueringsprosessen. Svar:

4.5	**Teori**: Se sikkerhetsloven **Spørsmål**: Har dere som tilsynsmyndighet erfaring om bedriften har en prosess for risikorapportering som inngår i grunnlaget for evaluering av sikkerhetstilstand? **Hensikt**: Hensikten med spørsmålet er å undersøke om bedriften har en prosess for risikorapportering som inngår i evalueringsprosessen. Svar:

4.6	**Teori**: ISO27014 **Spørsmål**: Har dere som tilsynsmyndighet erfaring om bedrifter har satt krav til hvilke evalueringer som skal gjøres i ulike deler av organisasjonen? (hva skal evalueres) **Hensikt:** Hensikten med spørsmålet er å undersøke hvordan bedriften innhenter datagrunnlag for evaluering. Svar:

4.7	**Teori**: ISO27014 **Spørsmål**: Har dere som tilsynsmyndighet erfaring om hvem i bedriften deltar i evaluering av status før ledelsens gjennomgang? Og hvem deltar i ledelsens gjennomgang på øverste nivå? **Hensikt:** Hensikten med spørsmålet er å undersøke hvilke interessenter som er direkte involvert i underlaget for dialogen med styret. Svar:

4.8	**Teori**: ISO27014 **Spørsmål**: Har dere som tilsynsmyndighet erfaring om hvor ofte de ulike bedriftene gjennomfører evaluering? **Hensikt:** Hensikten med spørsmålet er å undersøke hvordan bedriften jobber med evalueringsprosessen. Svar:

4.9	**Teori**: ISO27014 **Spørsmål**: Har dere som tilsynsbedrift erfaring om hvordan de ulike bedriftene dokumenterer evalueringsprosessen? **Hensikt:** Hensikten med spørsmålet er å undersøke hvordan bedriften jobber med evalueringsprosessen.

4.10	**Teori**: ISO27014 **Spørsmål**: Har dere som tilsynsbedrift erfaring om hvem i bedriften som blir orientert om resultatet av evalueringsprosessen/årlig evaluering? **Hensikt:** Hensikten med spørsmålet er å avdekke ulike ansvarsområder i bedriften når det gjelder evalueringsprosessen.

Kategori 5: Forholdet til styret

5.1	**Teori**: ISO 27014 **Spørsmål**: Har dere som tilsynsmyndighet erfaring om hvem som har dialogen med styret?

	Hensikt: Hensikten med spørsmålet er å kartlegge og avdekke ulike ansvarsområder mellom styret og sikkerhetsledelsen.

5.2	**Teori**: ISO 27014 / PWC styreboken **Spørsmål**: Har dere som tilsynsmyndighet erfaring om hvilken rolle styret har i sikkerhetsstyringen? **Hensikt**: Hensikten med spørsmålet er å undersøke om i hvilken grad styret engasjerer seg aktivt i fastsettelse av retning og evaluering av effekter av investeringer og tiltak.

5.3	**Teori**: ISO 27014 **Spørsmål**: Har dere som tilsynsmyndighet erfaring om hvordan evalueringsprosessen følges opp med styret? **Hensikt**: Hensikten med spørsmålet er å undersøke ulike prosesser og løsninger for å sikre styrets involvering, interesse og forståelse for sin rolle knyttet til sikkerhetsstyring.

Appendix D

Sector specific analysis

The complete sector specific analysis of the companies.

Sector specific analysis of the companies

Category 1

In the public sector, only one company has defined both a management system and security governance. There is still another business in the public sector that has defined a management system but lacks a clear definition of security governance. The remaining enterprises in the public sector do not have a clear definition of a management system or security governance but have this mentioned in their management policy for information security. Only one of the private sector companies has defined a management system and security governance. Here, too, it is mentioned by several businesses that although there is a lack of a clear definition of a management system and security management in the company, this is nevertheless made clear in their management policy for information security.

Businesses in the public sector use frameworks based on, among other things, NIST, NSM's Basic Principles for ICT Security, and the ISO family, of which ISO 27001 is mentioned by four businesses specifically. Only one company in the public sector uses a framework based on ISO 27014. One of the companies in the public sector further informs that their Information Security Management System (ISMS) is based on ISO 27001. The companies in the private sector also use a framework that is based on NSM's Basic Principles for ICT security, ISO, and NIST, two of which mention the NIST Cybersecurity Framework specifically.

In the public sector, only one company uses the processes "direct", "monitor", "evaluate", and "communicate". In the private sector, two companies use the five processes "Identify", "Protect", "Detect", "Respond", and "Recover" mentioned in the NIST CSF. Furthermore, two businesses in the private sector mention that they do not use any specific processes other than the PDCA circle. In the private sector, only one company informs that they will implement and make a typical "copy-paste" of the various management processes in the management model in the ISO 27014 framework. However, these concepts are only currently known in the business.

Other than `Kraftberedskapsforskriften,' which mainly applies to the power and energy sector, as well as the financial regulations, which apply to all public agencies, there are no other sector-specific laws and regulations that set requirements for the evaluation process and the board's responsibility for safety at the various businesses.

Category 2

In the public sector, all businesses have carried out a value assessment, of which six of seven enterprises explicitly mention that their values have been assigned a respective criticality. More than half of the businesses in the public sector have a valuation of their overall values. In the public sector, a company explicitly mentions that they have built up a valuation system where the type of information contained in that system, consequence, criticality, control of data processing agreements, and more are mapped. In the private sector, all the businesses have carried out a valuation, where over half have carried out an overall valuation of the business's intangible assets and supporting IT services/processes to take care of the CIA.

In the public sector, essentially all businesses respond that their values are assessed and determined in the directors' meeting/superior management, where these values are included in the risk matrix so that risks are assessed against these values. A business within the public sector explicitly mentions that its values are run through a so-called rating system where you answer x number of questions to find the pain threshold and their respective criticality. In the private sector, there is more mention of its processes and standards for decisions and determining values in the business. Two out of seven firms in the private sector inform that the values are categorized according to defined threshold values and are grouped according to overall categories of personnel, locations and facilities, market, concessions, services, information, and data, where each group has further subgroups. A business explains that its values are determined in a structured matrix where value is measured in terms of business criticality.

Six out of seven businesses in the public sector have set targets for information security. On the other hand, there is more variation in connection with whether these goals are at an overall or more profound level. The one business in the public sector, which also uses the ISO 27014 framework, uses one of the management processes "direct", which the business calls "goals and results management", where they have long-term strategic goals that are broken down into operational and annual goals that are revised annually. Another business in the public sector informs that they have a stated goal for information security and the CIA, but this is not quantitative enough to evaluate/measure. This does not apply to businesses that have not set information security goals.

In the private sector, all businesses have set goals for information security. Still, here too, there is variation as to whether these targets are at an overall or more profound level. Over half of the businesses in the private sector have overarching goals, with the majority mentioning that these are in their policy for information security. In contrast, only three firms have goals that are elaborated in associated underlying policies. One of these three companies mentions that their security goals are organized according to the NIST CSF. In contrast, another company informs that its security goals are linked to establishing controls integrated into its so-called risk management.

In both the public and private sectors, it is common for most businesses to use key performance indicators to determine whether the set goals for information security have been achieved and/or are possible. It is further informed that these KPIs are used as far as possible, as not all the goals are equally measurable in the individual business. In the public sector, a company elaborates that information is obtained through the monitor and evaluate process where they carry out information retrieval/control. Furthermore, a self-assessment of the safety of the various business areas is carried out, which is reported to the management, where a new assessment is made based on whether something has been achieved or not. In the private sector, three businesses explicitly mention that, in addition to established KPIs at the group level, various processes are used to measure and monitor whether or not the goals are achieved using a framework. NSM's Basic Principles for ICT Security and NIST CSF are particularly emphasized here. Furthermore, two businesses in the private sector use maturity measurement according to ISO 27002.

Category 3

Two companies in the public sector describe the evaluation process where target achievement is assessed, whether this was good enough, or whether these targets need to be adjusted and/or corrected. They further explain that what is included in this process is information that has been collected through functions, conversations with support functions, collaboration with IT, follow-up of control activities, etc. This is then collected in forms, and professional assessments are made of what is also discussed with the management line and whether it requires changes and/or is potentially made by the various identifications. Three businesses explain that the evaluation process works in an unclear and unsystematic way and that improvements are desirable when it comes to the evaluation process of information security. Two of these three businesses further explain that this is already being improved in the company. Another company explains that what is included in the evaluation process is unknown. Still, that control and evaluation of information security are carried out, as well as internal control, technical vulnerability tests, risk assessments, and more. This business also points out the evaluation process as an area for improvement. The last company performs the evaluation process at several levels, where reports and corrections are carried out if deviations are detected.

In the private sector, three businesses inform that the evaluation process takes place in the management's review. Certain evaluation criteria must be made in various business areas where maturity, challenges, and proposed measures are described. This must also be assessed concerning the general risk and threat picture of what should be emphasized. Another company explains that they use a framework in the evaluation process to follow up the goals set and given by the same framework, the NIST CSF. This is carried out in workshops where spreadsheets are used for mapping and evaluation. Furthermore, another company explains that previously no work has been done with the evaluation process and that this has taken place to a minimal extent, but that this will now be improved. The last business informs that they have not defined an evaluation process but rather a GAP analysis against NSM's Basic Principles for ICT security, where follow-up and prioritization are carried out.

Among businesses in the public sector, the basis for management's review is essentially the same. More than half of the companies informed that the basis for management's review is linked to the award letter, which includes several sub-elements such as maturity assessments, incidents, risks, the threat and situational picture, and external audit and supervision. A business in the public sector points out that the management's commitment is a problem as this is not good enough. In the private sector, half of the businesses answer that management's review is about reporting the status of work with information security in light of set goals and ambitions, as well as risks and the threat picture. The basis for management's review is therefore further answered with various sub-elements that are included, such as separate reports, risk status, the situation and threat picture, and more. A business informs that the basis for management's review deals with the general threat picture for the current year but mainly concerns vulnerabilities and, to a small extent, information values in the company.

A company in the public sector has a form of CISO organization instead of a separate role for the CISO. The CISO organization is divided into IT cyber and IT information security. The information security department is, among other things, responsible for awareness, responsibility, and evaluations, while the cyber department is responsible for securing technical information. At another company, the responsibility lies with the managing director and designated executive vice president for tech, who point to the CISO. Two other companies explain that the responsibility lies with the IT director, who has a link to the CISO. At last, one company explains that the responsibility lies with the CEO, who is responsible for information security. He gives assignments to the security manager who has a direct reporting line to the CEO but is organized within the finance department director. In addition, the business has a digital security function in the IT department that reports directly to the technology director and is professionally followed up by the security management function. The security manager leads the security management function.

Several businesses in the private sector use the line distribution for how the company has organized responsibility for information security, where the CISO and its resources are defined as the second line. One company explains the organization where the CISO is placed at the CIO office along with the IT security manager in his department with the intended two employees. They also use key roles in the organization with responsibility for security within their respective areas of responsibility. Furthermore, another business in the private sector explains that there is responsibility for security in each business area, and they then have overall responsibility for themselves. There are also three levels where the CISO is the group responsible for security, who is also the head of security. The CISO has overall responsibility for the group, while the director has responsibility for those in his business area. Some security objectives for which all employees are responsible are also explained.

Two companies in the public sector inform that the person who gives assignments to the CISO or equivalent is the CSO, where dialogue meetings are held between them periodically. Two other companies inform that the company's board gives the assignment to the CISO/CSO or equivalent. Furthermore, another company explains that it is rooted in the manager's downward organization of responsibility. The CISO is placed under the IT director, and the CSO under another director, and we collaborate on this. Another business informs that the assignment is given by their labor and welfare director to the safety manager, who has a reporting line back to their labor and welfare director. The latter business explains that no specific role gives assignments to their CISO/CSO or equivalent as their department delivers this. The assignment is delegated through structure, the board, CEO, and other directors to the CISO.

Among the businesses in the private sector, four companies inform that assignments are given by the board and management to the CISO/CSO or equivalent. It is also mentioned that this can be given by the chief of staff and the group management of another business in the private sector. The general manager and IT manager are also designated as roles that give assignments to the CISO in another company. The last industry explains that the assignment is given by top management or the person assigned by top management. It is further informed that assignments are often implemented following CISO recommendations based on e.g., inspections and audits, changes in the risk and threat picture, or deviations from laws and regulations.

Where and in what role the responsibility for evaluating the state of safety and achieving targets lies between the public sector businesses. Two companies inform that this responsibility lies with the CEO at the top management level, which further delegates down the hierarchy. Two other companies explain that the responsibility lies with the CISO. One specifies that this is done in collaboration with the CSO, where both participate in a comprehensive report of all security areas. Furthermore, another business informs that they have an overarching policy that the CSO has for all its management systems, which sets requirements for each one. But within each individual, there will be specific goals that are defined, and they are anchored with the business strategy, and everyone must decide this. The last two companies explain that the responsibility lies with the security manager and the security section, where one company specifies that the evaluation itself must be carried out by those responsible in the line. The businesses further explain that they are working to have it incorporated that they have evaluation/management reviews at each departmental level - then they will have a better basis for knowing their security situation.

In the private sector, five companies inform that the responsibility for evaluating the state of security and goal achievement lies primarily with the CISO at the top management level, of which one company specifies that this responsibility is shared with the Security Manager at the company level. Furthermore, another business in the private sector explains that responsibility is placed in the first line. They further explain that the second line can evaluate the first line's evaluation. Still, it is not the second line that actually evaluates the state of security and goal achievement. The last business informs that the responsibility lies with the staff.

Two enterprises in the public sector inform that they use CSO as other control functions to follow up on the status and basis for evaluation. Another business informs that they make use of the group audit. Furthermore, another company explains that they have safety coordinators in the lines, i.e., in counties and performance areas. These are called support functions that look after and report to the security section if they see errors and deficiencies that need to be followed up. They also have a function in IT called digital security which follows up more technical security. Another business informs that they use data protection representatives and external audits. The latter industry replies that they use risk management and internal control functions to get input and support.

In the private sector, four businesses mainly use internal and external audits as other control functions to follow up on the status and basis for evaluation. Furthermore, another company explains that their second line functions as a control function and that they make use of it. At another business, it is explained that they use a Data Protection Officer (DPO) who will, from their point of view, evaluate security related to privacy regulations. The latter company informs that they do not use control functions other than the CISO to follow up on the status and basis for evaluation.

Four companies in the public sector inform that the company obtains information/reporting from the various operational functions to those responsible for evaluation through interviews, reports, established services, and their part. Here, one in four businesses further explains that they have everything stored and handled in a tool where a dashboard with mandatory processes is created. Another company explains that they have a goal and result management process. Here they have something called reporting packages which are part of tertiary reporting where they report three times a year. The business also has something called a security support team that goes out and visits the companies to gather impressions and situational awareness. Furthermore, another business explains that information/reporting is brought in through predefined monitoring solutions with dedicated technology, statistics from pentest, asset management systems, and privacy-related manual reports.

Three businesses in the private sector inform that they are using the ServiceNow tool to gather information/reporting from the various operational functions to those responsible for evaluation, where one of these businesses further points out a desire for greater use of indicators. Another company explains that they mainly use reports, audits, and evaluations according to frameworks. The remaining businesses inform that they do nothing other than report on sent questions to collect information from the various operational functions but that there is a desire for greater use of key performance indicators (KPIs) and benchmarking.

Category 4

Five companies in the public sector confirm that they have defined indicators for goal achievement in their company. One of these five businesses explains that these indicators are only defined for the six security goals they have set. Another of these five businesses informs that they have defined indicators for the annual goals. Still, in the long-term strategic ones, the business is working on setting measurement criteria here. As with risk management, the company must introduce indicators to evaluate risk against prioritized values. This is to revise the risk management so that it is in accordance with 5814. The remaining businesses inform that they have not defined indicators for goal achievement but that they still have an indication of where they should be.

Also, in the private sector, five companies have defined indicators for target achievement in their company. Nevertheless, a couple of these five businesses pointed out that only indicators have been defined for the annual and overarching goals, and not necessarily all of them. The remaining two businesses explain that they have no concrete indicators for goal achievement apart from technical KPIs, explains one company. Several businesses in the private sector point out that they are working on developing sound and establishing measurement indicators.

Whether the various businesses in the public sector use any tool to secure data basis and assess the effects of activities and measures, four businesses explain that they mainly use Microsoft Office tools such as Excel, Word, and PowerPoint. Two other companies explain that they use ServiceNow. Furthermore, another business explains that they are using an Enterprise Risk Management tool. In the private sector, two businesses use ServiceNow to secure data basis and assess the effects of activities and measures. Three other companies in the private sector further explain that they do not use any specific tool but that one of these three businesses plans to introduce ServiceNow. Another company informs that they only use KPIs and OKRs to define targets and assess effects, while the last company explains that they only use the SIM tool as a basis for their deviation system.

In the public sector, five businesses respond that they think there is a suitable amount of access to relevant tools to evaluate and report on the state of security but that many of these may become large and complex for several of the businesses to be able to implement. It is also mentioned that knowledge and understanding when using such tools make this a challenge for several industries. Only one company describes access to relevant tools as poor and that this should be better. There is also only one business that is satisfied with access to appropriate tools without justifying this further.

In the private sector, two businesses respond that they think access to relevant tools to evaluate and report on the state of security is poor. One of these two businesses further explains that even if they use ServiceNow, this is not the best tool to use in connection with evaluating and reporting the security state, even if the tool does this. Four other businesses in the private sector inform that they are either unsure or think that there is a suitable amount of access to relevant tools, but that these tend to be a challenge as they are large and complex. Only one business replies that they think there is good access to relevant tools without justifying this further.

Six businesses in the public sector inform that they have a process for non-conformity reporting. On the other hand, only four further specify that non-conformance reporting forms part of the basis for evaluating the safety situation. Only one business in the public sector does not have a deviation process that forms part of the basis for evaluating the state of safety. They further justify this as a conscious choice made by the tech department. Six businesses in the private sector inform that they have a process for non-conformity reporting that forms part of the basis for evaluating the state of safety, of which one of these six businesses explains that this is a principle in their governing documents and that this is a requirement. Also, in the private sector, only one company does not have a process for non-conformance reporting but further informs that they have technology that can retrieve this.

All the businesses in the public sector respond that they have a process for risk reporting that forms part of the basis for evaluating the state of security. This also applies to all businesses in the private sector. Only one company in the private sector answers that they are quite weak in risk management, both in terms of operational risk and security risk. It is further explained that nothing is working in the governing. There are no requirements for how risk should be assessed, where it should be assessed, and how it should be reported, handled, and aggregated.

In the public sector, six businesses respond that they have set requirements for which evaluations are to be carried out in various parts of the organization, i.e., what is to be evaluated. Several of these businesses explain that this is carried out systematically, where there are procedures around risk and internal controls to achieve a reasonable level. Only one company in the public sector replies that they have not set requirements for which evaluations are to be carried out in various parts of the organization but that the teams themselves must evaluate the security in their areas and services. In the private sector, four businesses respond that they have set requirements for evaluations to be carried out in various parts of the organization. One of these businesses explains that they use a Security Governance Framework that allows them to control. Furthermore, three other companies respond that this is done partially as assessments are carried out of various IT projects and the like, but no specific requirements have been set.

Six companies in the public sector answer that it is mainly those with professional responsibility for safety who participate in the evaluation of the status before management's review, where a report is drawn up which is anchored by those responsible for it. One of these six businesses further informs that the risk management function will also be involved. Who participates in the management's review at the top level, all six of these businesses answer that this mainly includes the group management and top management. It is also mentioned by some specific businesses in the public sector that information security manager, general manager, and CSO are also other roles that participate in management's review.

It is a business in the private sector that responds that their Enterprise risk management is reported to the corporate management board (CMB) through a written note and a presentation. This is reported from the management to the board. The business further informs that they have a steering committee where the CIO agrees on what is desirable to report across the business areas. The CIO and CISO attend the group management, where they participate in the management's review. The remaining six companies in the private sector also inform that the CISO, the group management, and the board participate in the management's review at the highest level. It is further explained that it is mainly key people and those responsible for security who participate in evaluating the status before management's review.

In the public sector, four companies carry out the evaluation process once a year. Only one company answers that this is carried out every six months as a minimum. Furthermore, only one company responded that this is carried out quarterly at the top level, monthly at the operational level, and weekly at the incident level. Only one business in the public sector does not carry out an evaluation process. Five companies in the private sector conduct the evaluation process once a year. Furthermore, two businesses answer that they carry out the evaluation process every six months.

Three businesses in the public sector respond that the evaluation process is documented and described in Excel, Word, and PowerPoint. Another company also explains that this process is documented primarily in a support system, but they also use Word and PowerPoint. Another business informs that this process must be documented in a case management system but has not been done. Furthermore, another company explains that this process is documented in MIME and is open to inspection by the public. Only one company does not document the evaluation process in the public sector as they do not carry out this process at all.

Five businesses in the private sector respond that the evaluation process is documented in forms and documents, of which three of these businesses specify that this is done in Word and PowerPoint. Furthermore, another business in the private sector explains that this process is documented and described in their respective systems, ServiceNow. There is only one company that is unsure where and whether the evaluation process is documented at all.

In the public sector, five businesses respond that those who are informed about the evaluation process/annual evaluation results are those who participate in the management's review, the group management, and the board. A couple of companies also inform that this information is also given to various directors and safety coordinators around the company. Only one business in the public sector answers that this information is open and available to everyone. Furthermore, only one company does not inform about the result of the evaluation process as they do not carry out this process in their business.

In the private sector, six businesses responded that those informed about the evaluation process/annual evaluation results participate in the management's review, i.e., the CFO/CEO, the group management, and the board. A business also informs that this information is also given to the internal audit. Only one company in the private sector informs that this information is released to the general manager and IT manager.

Category 5

In the public sector, three companies inform that their CISO/CSO is responsible for information and dialogue with the board about the security situation. Furthermore, there is a company that explains that it is the technology director who is responsible for information and dialogue with the board, but that this must be done in accordance with the CISO. Another company explains that the company's general manager is responsible for the dialogue with the board but that this must also be done in accordance with the CISO/CSO and the risk management function. It is further informed by another business that they have two organizations behind it, IT cyber and IT information security, where the head of staff at IT information security is responsible for information and dialogue with the board in accordance with the CEO. The latter explains that they use a separate unit under the Ministry of Transport responsible for the dialogue with the board.

In the private sector, five companies inform that it is mainly the CISO and/or CEO responsible for information and dialogue with the board about the security situation. Of these five businesses, two further explain that this is done according to the CEO. In contrast, another business informs that this can be done in accordance with the executive vice president for data and technology. Another company explains that it is the steering committee, together with the CFO/CIO, who is responsible for information and dialogue with the board. Furthermore, the latter business explains that its CISO has no role vis-à-vis the board.

Regarding the board's role in security governance, two companies inform that there is a close dialogue with the assignment/award letter. Here, one of the two businesses further informs that the board is engaged and gives an annual assignment to follow up with dialogue and reports for each term to ensure compliance with the Safety Act. Three businesses explain that the board's role in safety management is mainly based on their role as supervisor, where they must ensure that the business is in line with the guidelines and set speed and direction for the strategy. Of these three businesses, one explicitly mentions a desire for more reporting. The latest activity informs that the board is the one who determines overall policy and seems committed and supportive. Only one business in the public sector does not know what role the board has in safety management. A total of 4 out of 7 enterprises comment that knowledge and culture are considered a challenge by the board.

In the private sector, two businesses inform that the board's main task is to ensure that the owners' interests are safeguarded. This includes ensuring that the business fulfills the duties imposed by law and regulations, that the business's values are secured, and that the business operates within an acceptable level of risk. Furthermore, another company explains that the board has an overall responsibility as set out in the board instructions, where the board owns risk appetite and criteria. It is further informed that the board participates primarily in any investments with the management. Two other businesses explain that the board is one of the policymakers for security, where they set good requirements and a good agenda for the safety work in the business. Another business has a foreign owner, and reports are therefore carried out to a foreign CISO, but no further mention is made of the role of the foreign CISO and the board. The latest business informs that the board is concerned that there should be sufficient security in the industry but points out uncertainty and a lack of maturity on the part of the board.

A business in the public sector replies that they do not know whether or how the evaluation process is followed up with the board. The remaining companies informed that the evaluation process is followed up with the board through reporting that either takes place quarterly or twice a year, of which three businesses explicitly mention that it could have been more systematic. They further informed that it is difficult to find the right level of what is to be dealt with as a lot is raised and brought up to the management. In other words, the threshold is too low for submitting things to management. Two businesses in the private sector also said they do not know whether or how the evaluation process is followed up with the board. The remaining companies inform that the evaluation process is followed up with the board through reporting and presentation, but no one mentions how often. In the private sector, a business expresses a desire for the evaluation process to be followed up with the board in a better and more systematic way, as the follow-up currently takes place more ad hoc.

Appendix E

Controlling authorities analysis

The complete analysis of the controlling authorities.

Analysis of the controlling authorities

Category 1:

The four controlling authorities interviewed about their experiences of whether the various businesses within the public and private sectors have defined security governance and/or management systems responded mainly that they feel very few have a written definition. They nevertheless inform that they have gained experience that most businesses have come to terms with the meaning of the various definitions.

All the controlling authorities inform that, in the main, they see that most businesses use a system and/or a framework for managing information security. They further explain that, on the other hand, they do not set any specific requirements for which framework the various businesses must use and that this is optional for each individual company. It is mainly ISO 27001 that they have gained experience with that the different companies either adopt in whole or in part or draw inspiration from this. They are also familiar with NSM's Basic principles for ICT security among many businesses. Still, on the other hand, they see a smaller number of companies that use NIST CSF and ISO 27014. They only mention a couple of businesses that they are familiar with that use either entirely or part of ISO 27014.

To the next question, they answer that they have gained a little experience with the businesses being familiar with the processes "monitor", "direct", "communicate", and "evaluate" that are part of the governance process. This is also precisely because they have gained little experience experiences with businesses that make use of ISO 27014. It is further explained that very few use these words but use similar processes when using other frameworks. They inform that they are more familiar with the companies' use of PDCA and the five processes included in the NIST CSF, namely "identify", "protect", "detect", "respond", and "recover".

None of the controlling authorities use ISO 27014, but one controlling authority specifies that they are aware of it and follow it indirectly. Only one controlling authority answers that they measure up against ISO 27014, but this is done indirectly where they check against criteria that are subject to supervision.

The controlling authorities list essentially the same laws and regulations that the various businesses are subject to as the companies themselves. The Emergency Preparedness Regulations, the Security Act, the ICT Regulations, the Financial Enterprise Regulations, and the Financial Regulations are the laws and regulations the various businesses are subject to and set requirements for the evaluation process and the board's responsibility for security. The Financial Regulations, the Power Contingency Regulations, and the Security Act are essentially sector-specific rules that various businesses must comply with.

Category 2:

If the various businesses have an overview of the values in the business and their respective criticality, the various controlling authorities learn that this is generally done but that, on the other hand, there are differences in how detailed this is. One of the controlling authorities explains that they have primarily gained experience that the various businesses have an overview of their overall values . This is done to a greater extent than previously, but this is still a problematic area with major shortcomings and a high potential for improvements. The controlling authorities experience, to a greater extent, that the various businesses have an overview of their values and their respective criticality, where two of these further explain that this is required by law. They nevertheless explain that they experience a large variation in how well the various businesses justify valuation and that there is a clear distinction between the large and smaller businesses. It is further explained and made visible to all controlling authorities that competence and culture create difficulties for the various businesses and the understanding of how the various values can be misused.

All the controlling authorities respond that they experience, to a large extent, that the various businesses have some set goals for information security but that this is very general for most companies. They further informed that only a small number of businesses break down these overall goals into specific sub-goals and that it will therefore be difficult for many to assess whether they have achieved the various goals as they are too large and overarching. According to the Security Act, adequate security must be achieved for the national security interests of the business, which must be protected by each individual business. Very few follow up on this in detail - whether they have an action plan or follow-up plan and whether they break down the overall goals into a single activity, explains one controlling authority.

How the various companies determine whether the set goals have been achieved and/or possible, one controlling authority, in particular, learns that they have a couple of examples of NIST being used and maturity measurement/benchmarking on this. They further explain that assessing whether the measurement is within/outside that tolerance is difficult, as it quickly becomes a bit subjective. They have seen many who have done this in good ways but inform that the quality may not always be as good and that many overestimate their own knowledge. Another controlling authority learns that they see that many people have a follow-up plan but do not follow it up. The degree of goal achievement varies as many people have a plan that is not always followed up, and if it is carried out, there is little control over whether the measures are reasonable, and if the measures are not good enough, they may not have implemented improvement either. The controlling authority further explains that to obtain proper security, the business must have implemented effective measures. Many have goals for what they will do, but not what they have brought about in terms of security – this is a common finding, explains the controlling authority. The controlling authority concludes by saying that they want the businesses to have a greater emphasis on implemented measures and goal management linked more to goals and measures but sees that this is in great short supply.

Category 3:

How the various businesses work with the evaluation process and what is included in this process, one of the controlling authorities learns that the process itself is poorly defined and is not connected to the goals, as many are not aware of measuring risks, incidents, and those that have major audits, etc. They also experience that the level is often set further down than in the management system. One of the controlling authorities specifies that they see that the businesses carry out security audits and controls of the company and that many do this in a good way. Nevertheless, it is experienced that they see measures that must be implemented following the management's review, but that this is to a small extent fulfilled as they see the comprehensive measures every year. Here, another controlling authority points out that they have the most and best experience with the larger enterprises where they use control frameworks and that the evaluation process is carried out in a structured and thorough manner.

All controlling authorities are generally aware that the basis for the management's review of the various businesses is based on the business's goals and what they have worked on in the previous year. This usually includes risk assessment, deviations, incident management, and preparedness.

The controlling authorities experience something different in how the various businesses have organized responsibility for information security. It is further explained that they generally feel that most companies have a security organization with a security manager. It is also pointed out that many companies use line distribution. Still, it can be experienced differently when the various companies have chosen to place the CISO in the line distribution. It is also explained that the security person can also be exempt from the line, some of which have this role placed in the staff.

Whoever assigns assignments to the CISO/CSO or equivalent at the various businesses replies to the controlling authorities that they often experience that the mandate of the CISO/CSO has been given and that much is self-managed within each business. It is often rooted from the management downwards in the organization of responsibility in most companies.

The controlling authorities reply that the security manager is mainly responsible for evaluating the security situation and achieving goals at the individual business. One of the controlling authorities further informs that many companies have also entrusted this role to the line, where the line reports to the security management.

All the controlling authorities explain that if the various businesses use control functions other than the CISO/CSO to follow up on the status and basis for evaluation, this primarily uses internal audits where security and other elements are included. Consultants are often hired here, but this can vary from company to company. External consulting firms and controlling authorities are also used.

The various businesses use several different reporting mechanisms to obtain information/reporting from the various operational functions to the person responsible for evaluation in the company, explains one of the controlling authorities. Generally, all controlling authorities experience and experience that it is through reports that the various companies obtain information. One of the controlling authorities further points out that there is and is experienced little systematic information gathering.

Category 4:

The controlling authorities have little experience with whether various businesses have defined indicators for goal achievement. One of the controlling authorities explains that it is experienced that several companies have this, where they often look at SLA requirements in the form of uptime, quality, changes, etc.

ServiceNow, Remedy, and Jira are examples of tools for evaluating and reporting the state of security that one of the controlling authorities experiences that businesses are using. Some of the controlling authorities also see some use of these tools, but that it can be experienced by the individual business as complex to use and that they, therefore, rely on more standard reporting tools. They further inform that they do not feel many companies have KPIs in security areas.

There are some differences between the controlling authorities if they find that the businesses think there is good access to relevant tools to evaluate and report the state of security. One of the controlling authorities finds that the companies have good access to appropriate tools. One of the controlling authorities answers somewhat more uncertainly as they inform that it is not certain that all businesses know all the offers and which device is most suitable. They further specify that having a better overview of access to this would have been desirable.

All the controlling authorities reply that it is required for all businesses to have a process for non-conformance reporting which forms part of the basis for evaluating the state of security. However, the extent and level of this done varies between the businesses. It has also been experienced that some companies lack this. All the controlling authorities also reply that it is required for all businesses to have a process for risk reporting which forms part of the basis for evaluating the state of security. Still, there is also variation in implementation and to what degree and level this is done. Here, too, it is pointed out that this is several businesses' improvement potential.

A couple of the controlling authorities have little experience with whether companies have set requirements for which evaluations are to be carried out in different parts of the organization other than the line distribution and their assigned tasks. It is further mentioned that companies are required to have sound corporate governance. The final controlling authority also replies that companies must always risk assessing the means and/or solutions they use. According to the GDPR, four risk assessments must be in place, explaining the controlling authority.

From who participates in the evaluation of status before management's review and who participates in management's review at the highest level, the controlling authorities learn to a large extent that it is the security function and key persons, functions, and service owners who participate in evaluation before management's review. They further reply that they experience that it is almost always the management team, the security manager, and sometimes the operations manager who take part in the management's review. A subset of the board and/or a representative from the board is also known to participate in the management's review but to a lesser extent.

All the controlling authorities reply that they know that the companies conduct the evaluation process once a year. One controlling authority specifies that those subject to the Security Act are required to do this at least once a year but that they rarely find that it is carried out more often than this.

How the companies document the evaluation process, the controlling authorities experience that what they see is that all security reports and checks or audits are mostly done on a Word and Excel basis. Some have risk management tools and deviation tools and create reports from these with some graphs where these are included in the annual evaluation and annual report.

The controlling authorities experience that those informed about the annual evaluation results are the top management team with a manager. One of the controlling authorities further explains that senior management reports to the ministry as this is a requirement in the award letter. One of the controlling authorities points out that the security organization is also usually informed of the annual evaluation results, but this is not necessarily communicated well enough to the rest of the business.

Category 5:

The controlling authorities explain that they mostly find that the business manager or those who deal with business management are responsible for information and dialogue with the board about the security situation. It is further learned that the responsibility for information and dialogue with the board about the state of security lies primarily with the IT director, managing director, and/or information security manager at the companies that have a board, while the companies that do not have a board relate to the ministry.

All the controlling authorities explain that there has been a perceived absence of what role the board has in security governance but that the companies have become more and more aware of their responsibilities, especially after the significant events that have occurred during the last few years where the attack on the Stortinget and Østre Toten is taken up as an example. One of the controlling authorities further informs that there is increased reporting in the reporting area, but that information security is problematic. They further explain that they experience that several boards are struggling to get people with sufficient knowledge in this area.

How the evaluation process is followed up with the board among the various businesses, the controlling authorities have gained a little experience. They explain that they mainly experience that reports are presented on the annual status of information security and privacy, preferably in a document summarizing how they have worked in the previous year, including deviations and more. A controlling authority replies that it is difficult to answer but experiences tremendous variation in quality where the larger businesses are better than the smaller businesses.

NTNU

Norwegian University of
Science and Technology