

**UNIVERSITY
OF OSLO**

Dinh Uy Tran

**Holistic Understanding of
Information Security Posture**

Thesis submitted for the degree of Philosophiae Doctor

Department of Informatics
Faculty of Mathematics and Natural Sciences

Sykehuspartner Trust



2023

© **Dinh Uy Tran, 2023**

*Series of dissertations submitted to the
Faculty of Mathematics and Natural Sciences, University of Oslo
No. 2696*

ISSN 1501-7710

All rights reserved. No part of this publication may be
reproduced or transmitted, in any form or by any means, without permission.

Cover: UiO.
Print production: Graphic center, University of Oslo.

Summary

As part of the literature search for the present study a vast amount of literature related to information security governance and management was found to exist. However, these contributions usually specify *what* to implement, but not *how* to implement, and especially *how* to gain an oversight of the information security posture (ISP). These contributions usually emphasise the importance of gaining management support and how to communicate in a way that the management understands, to ensure efficient security reporting. However, we found limited literature discussing how to actually communicate with executive management, while at the same time the literature usually discussed the importance of good communication. In addition, we found literature from the academic research sector and the industry which discussed the importance of integrating information security as a business element. However, these contributions did not discuss the practicability of this principle, while these studies usually discuss this from an information security perspective, and not holistically and integrated with business aspects. The goal of this thesis is to propose and describe an approach to strengthening information security governance (ISG) and reducing the gap between *what* and *how* to apply information security in a business setting. More generally, this thesis aims to support and extend existing research and industry frameworks.

First, we analysed existing research on *how* to organise an ISG program to gain an oversight of ISP while tailoring it to organisational differences. The main findings are that existing research and industry literature emphasises *what* to implement rather than *how* to do it, and does not focus on how to merge the ISG from standards to gain an oversight of ISP. Another interesting finding is that the literature interprets the concept of ISP differently and at different levels in the organisation, usually limited to an information security perspective and not holistically. As part of the present study, we have proposed a new definition of ISP that covers this holistically and at different levels, as well as a theoretical framework based on process management, to give ideas on how to organise an ISG program. In addition, we have developed strategies to identify and assess positive risks, in contrast to the traditional approach whereby information security has primarily focused on threats or *what can go wrong*. By including positive risk, ISG and risk management support a more holistic approach to information security and more ways to assess information security risk.

Next, we analysed existing research on the communication and reporting of information security activities. The main findings are that existing research and industry literature discuss the importance of speaking the same language as business, and that communication skills are important. However, these contributions typically do not discuss how to learn these skills related to

information security. We concluded that to speak the same language as management, future specialists should learn the relevant management fields and merge them with the information security field. We then proposed a theoretical framework for learning what we defined as Business Language for Information Security (BLIS). This framework includes key components with relevant sub-fields that an ISG specialist should learn, in order to communicate with executive management. In addition, we proposed strategies to communicate risk in four different ways. This can be used to communicate risk tailored to the risk perception of decision makers. This strategy includes positive risk, which is limited to research, although the new ISO/IEC 27005:22 has extended the definition to include positive risk.

Finally, in 2023, we published a textbook for information security management that considers our research results in greater depth, so that students can learn these fields. This book proposes a method to learn BLIS and includes in-depth learning material for different management fields. By learning the different management fields, future students can use this knowledge to understand organisational structure, corporate governance and process management related to information security, giving them the foundation needed to tailor the ISG program according to the organisation. The textbook, written in Norwegian, is already in use in two separate master's programmes at the University of Oslo.

Sammendrag

Som en del av studien er det blitt gjennomgått en omfattende litteratur, som omhandler styring og ledelse av informasjonssikkerhet. Et viktig funn er at bidragene som oftest spesifiserer *hva* som skal implementeres, men ikke *hvordan* i praksis, og spesielt *hvordan* man skal organisere for å få oversikt over informasjonssikkerhetstilstanden (eng. Information Security Posture - ISP). Som oftest peker disse bidragene på at det er viktig å få ledelsesstøtte ved å kommunisere på en måte som ledelsen forstår, og viktigheten av effektiv sikkerhetsrapportering. Vi fant mest litteratur som omhandler at det er viktig å etablere god kommunikasjon med ledelsen, men bare begrenset mengde litteratur som ser nærmere på hvordan man praktisk bør kommunisere med toppledelsen. I tillegg fant vi litteratur fra forskning og standarder som diskuterte hvorfor det er viktig at man integrerer informasjonssikkerhet som en del av virksomheten. Disse bidragene diskuterte ikke hvordan man i praksis kunne gjøre dette, og vanligvis diskuterte disse studiene problemstillingen fra et informasjonssikkerhetsperspektiv og ikke fra et helhetlig eller forretningsmessig perspektiv. Målet med denne avhandlingen er å foreslå tilnærminger og metoder for å forbedre informasjonssikkerhetsstyring (ISG) og redusere gapet mellom *hva* og *hvordan* for å bruke informasjonssikkerhet i et forretningsperspektiv. Avhandlingen støtter og utvider eksisterende litteratur fra forskning og standarder vedrørende styring og ledelse av informasjonssikkerhet.

Første trinn i studien var å analysere eksisterende litteratur fra forskning og standarder om hvordan man organiserer et ISG-program for å få oversikt over ISP slik at det er skreddersydd i forhold til organisatoriske forskjeller. Hovedfunnene var at eksisterende litteratur fra forskning og standarder legger vekt på *hva* som skal implementeres snarere enn *hvordan*. Samtidig finnes det ingen veiledning på hvordan man skal sammenstille og velge ut kravene fra ulike ISG-standarder for å få oversikt over ISP. Et annet funn, som var knyttet til begrepet informasjonssikkerhetstilstand, blir tolket ulikt og diskutert på ulike nivåer som samtidig er begrenset til et informasjonssikkerhetsperspektiv og ikke et helhetlig forretningsmessig perspektiv. Vi foreslår en ny definisjon av ISP som dekker det holistisk og på forskjellige nivåer, og foreslår videre et teoretisk rammeverk basert på prosessledelse for å gi ideer om hvordan man kan organisere et ISG-program. I tillegg har vi utviklet strategier for å identifisere og vurdere positiv risiko, for å utvide den tradisjonelle tilnærmingen til informasjonssikkerhetsrisiko som tradisjonelt fokuserer på trusler eller «hva som kan gå galt». Ved å legge til positiv risiko, støtter den en mer holistisk tilnærming til informasjonssikkerhet og åpner flere muligheter til å vurdere informasjonssikkerhetsrisiko på.

Studien har analysert eksisterende litteratur fra forskning og standarder om

kommunikasjon og rapportering av informasjonssikkerhetsaktiviteter. Hovedfunnene er at bidragene diskuterer viktigheten av å snakke samme språk som forretningen, og at kommunikasjonsferdigheter er viktig innenfor informasjonssikkerhet. Imidlertid diskuterer disse bidragene ikke hvordan man lærer disse ferdighetene med henblikk på informasjonssikkerhet. Vi konkluderer med at for å snakke samme språk som ledelsen, bør fremtidige spesialister lære relevante ledelsesfag og integrere disse med informasjonssikkerhetsfaget. Videre foreslår vi et teoretisk rammeverk for å lære det vi definerte som *Business Language for Information Security (BLIS)*. Dette rammeverket inneholder nøkkelkomponenter med relevante fagområder som en ISG-spesialist bør lære for å kommunisere med ledelsen. I tillegg foreslår vi strategier for å kommunisere risiko på 4 forskjellige måter. Dette kan brukes til å kommunisere risiko tilpasset beslutningstakernes risikooppfatning. Denne strategien inkluderer positiv risiko, som det finnes begrenset forskning og veiledning om, selv om den nye ISO/IEC 27005:2022 har utvidet definisjonen til å inkludere positiv risiko.

Studien har resultert i publikasjon av en fagbok innen informasjonssikkerhetsledelse som går mer i dybden på våre forskningsresultater, slik at studentene kan lære disse fagområdene. Denne boken foreslår en metode for å lære BLIS, og inneholder grundig læringsmaterieell for ulike ledelsesfag. Ved å lære de ulike ledelsesfagene vil man kunne gi godt grunnlag for fremtidige studenter til å forstå organisasjonsstruktur, styringsstruktur, prosessledelse og mye mer. Dette vil kunne gjøre dem i stand til skreddersy ISG-programmet tilpasset organisasjonen. Denne boken er pensum ved Universitetet i Oslo og blir brukt i det videre arbeidet med å validere og forbedre våre forskningsbidrag.

Preface

This thesis is submitted in partial fulfilment of the requirement for the degree of *Philosophiae Doctor* at the University of Oslo. The research presented here was conducted at the University of Oslo under the supervision of professor Audun Jøsang and associate professor Janne Hagen. The thesis is a collection of three papers and one book, presented in chronological order of writing. In addition, the thesis consists of an introductory section, followed by a summary of the papers, and finally a conclusion that relates them to each other. This work was supported and funded by Sykehuspartner Trust.

Acknowledgements

I would like to sincerely thank Audun Jøsang and Janne Hagen for their constant support and insightful discussions throughout this journey. I especially appreciate you both for giving me the freedom and trust to pursue my research interests. I want to thank all my colleagues in the Department of Informatics at the University of Oslo for their support and for hosting a book launch event, a day which I will never forget. Special thanks goes to Sykehuspartner for supporting and funding this PhD project, and of course to my colleagues for always supporting and cheering me on while I was absent from the office. Finally, I want to thank my family for always believing in me and encouraging me to pursue my dreams throughout this journey. Without the support of my family, I doubt I would have made it through the PhD programme.

This thesis marks the end of a chapter, but also the start of a new chapter of my life, and I am privileged and fortunate to be able to conduct research on topics that have become my passion. This PhD journey has helped my personal development and further affirmed that I will always pursue more learning, while ensuring that I use my knowledge to help others.

• **Dinh Uy Tran**

Oslo, November 2023

List of Papers

Paper I

Tran, Dinh Uy and Jøsang, Audun “Information Security Posture to Organize and Communicate the Information Security Governance Program”. In: *Proceedings of the 18th European Conference on Management Leadership and Governance*. (2022), pp. 515–522. DOI: 10.34190/ecmlg.18.1.729.

Paper II

Tran, Dinh Uy “Informasjonssikkerhetsledelse - En holistisk tilnærming”. Published by *Cappelen Damm Akademisk*, ISBN 978-82-02-75464-8. 236 s.

Paper III

Tran, Dinh Uy and Jøsang, Audun “Business Language for Information Security”. In: *Furnell, S., Clarke, N. (eds) Human Aspects of Information Security and Assurance. HAISA 2023. IFIP Advances in Information and Communication Technology, vol 674. Springer, Cham.*, pp. 57–68. DOI: 10.1007/978-3-031-38530-8_14.

Paper IV

Tran, Dinh Uy and Selnes, Sigrid Haug and Jøsang, Audun and Hagen, Janne Merete “An Opportunity-Based Approach to Information Security Risk”. To appear in: *The 4th International Workshop on Cyber-Physical Security for Critical Infrastructures Protection (CPS4CIP 2023)*.

Contents

| | |
|---|-----------|
| Summary | i |
| Sammendrag | iii |
| Preface | v |
| List of Papers | vii |
| Contents | ix |
| List of Figures | xi |
| List of Tables | xiii |
| 1 Introduction | 1 |
| 1.1 Motivation | 1 |
| 1.2 Problem statement | 4 |
| 1.3 Research questions | 5 |
| 1.4 Research strategy | 7 |
| 1.5 Structure of dissertation | 19 |
| 2 Contributions | 21 |
| 2.1 Summary of papers | 21 |
| 3 Conclusion | 31 |
| 3.1 Summary of contributions | 32 |
| 3.2 Future work | 35 |
| Bibliography | 37 |
| Papers | 42 |
| I Information Security Posture to Organize and Communicate the Information Security Governance Program | 43 |
| II Informasjonssikkerhetsledelse - En holistisk tilnærming | 53 |
| III Business Language for Information Security | 55 |
| IV An Opportunity-Based Approach to Information Security Risk | 71 |
| | ix |

Contents

| | |
|---|-----------|
| Appendices | 91 |
| A Appendix | 93 |
| A.1 Interview guide - Paper/book II | 93 |
| B Co-Author declarations | 97 |
| B.1 Paper I | 97 |
| B.2 Paper III | 101 |
| B.3 Paper IV | 105 |

List of Figures

- 1.1 Research strategy 7
- 1.2 Research method 10
- 1.3 Example - Coding 14
- 1.4 Example -Diagramming 16
- 1.5 Research project timeline 19

- 3.1 Summary of contributions 32

List of Tables

- 1.1 Overview - Research strategy. 8
- 1.2 An example of core categories from paper III. 15

Chapter 1

Introduction

1.1 Motivation

The source of my motivation for this PhD project is twofold: personal and professional. My personal motivation is related to my observations and experience from working in the healthcare sector. I had the opportunity and support from my employer Sykehuspartner Trust to be appointed as Chief Information Security Officer (CISO) for hire at Martina Hansen Hospital, from which I gained practical experience in the information security management field. I was fortunate to gain experience in organising information security structure and organisation, e.g. establishing and maintaining information security management systems (ISMS), information security management and governance, risk management and assessment, and business continuity. My experience as a special adviser at Sykehuspartner Trust was valuable, but through working as a CISO, I observed that something was missing, but could not grasp exactly what it was.

I received great feedback from colleagues during this assignment. I could, for example, explain and communicate information security in a way that the organisation understood, while gaining trust that I could ensure that information security could support business objectives. Another feedback was that I could adapt to organisational and decision-making structures while encouraging and motivating other key stakeholders in establishing an ISMS and governance structure. My colleagues from Sykehuspartner Trust were curious about my approach and wanted advice. I developed a structured approach through my experience and educational background. Well-recognised certification programs such as Certified information systems security professional (CISSP), CISSP-ISSMP (Certified information systems security professional-Information Security System Management Professional), Certified Information Security Manager (CISM) and Certified in Risk and Information Systems Control (CRISC) encourage information security professionals to speak the same language as the business, and for me this was natural, since I have a master's degree in IT and Management and a basic understanding of the management field that could help me understand and adapt to different organisational structures. Therefore, I could not give a direct answer to the questions from my colleagues because in every case, people and organisations are different. I joked to my colleagues that I could write a book and at that point I understood what was missing that I could not grasp earlier.

My assumption was that there is limited research and literature on the business element of information security, and my investigation confirmed my assumptions. Mostly, I found that the business element was important, but did not discuss *how* to apply information security in a business setting, as in my

1. Introduction

assignment as CISO for hire. This was one of the key triggers for starting to write my book *Informasjonssikkerhetsledelse - En holistic tilnærming/Information Security Management - A Holistic Approach* and served as the start of my PhD journey. The questions from my colleagues made me aware that there is not much literature on how to learn the business language and how to organise an information security governance program or ISMS specifically tailored for an organisation. This serves as my personal motivation for this PhD project.

My professional motivation is to support the healthcare sector in Norway and hope that my information security knowledge can contribute to the delivery of secure and reliable healthcare services. The healthcare sector has an emphasis on information security. There is, for example, a national strategy on e-health [5] to ensure a common strategy for digitalisation in the health care sector. The goal of digitalisation is to improve quality and effectiveness and provide healthcare services in new and improved ways. By 2030, the healthcare sector will have access to technology to support medical staff in providing more effective healthcare services, with easier access to patient data, regardless of where the patient lives in the country, and technology that can support medical staff in taking better decisions suited for their patients. These might be technology that enables home healthcare by bringing patients and medical staff closer, where the technology can monitor vital signs and enable secure communication between patients and medical staff. By monitoring patients' vital signs, medical staff can make well-informed decisions to provide the best medical service for the patient, with fewer visits and saving time. Another goal is to develop technology that enables secure and effective collaboration and sharing of patient data between different actors and sectors, and ensures that Norway as a part of the EU/EEA can share patient data when needed.

Based on these goals, there is no denying that information security plays a major role in enabling a secure way to share, store and process health data not only within an organisation, but also outside the organisation's boundaries. The national strategy on e-health [5] emphasises the following two areas that are fundamental to achieving the defined goals: 1) digital security/information security and 2) digital competence. The healthcare sector underlines that adequate information security is a condition for achieving the defined goals, since there has recently been a significant increase in severe cyberattacks in Norway and internationally, and a cyberattack could have severe consequences for the healthcare sector's ability to provide healthcare services safely.

This is not only an issue for the healthcare sector, but also for other public sectors, which is why the government has published a national strategy for digital security [19] which emphasises that the use of digital services needs to be secure and that organisations should digitalise in a sustainable way whereby cyber risks are appropriately balanced with security controls, and where organisations have the capability to manage security incidents if needed. Based on this, the Norwegian government underlines that the public sector needs to adopt a risk-based approach and use information security governance and management standards based on *best practice*. The government requires that the public sector has oversight over their information security governance program and that it is

aligned with organisational objectives, while ensuring that cyberattacks on a public organisation do not impact other organisations.

The Directorate of e-health, which is a subordinate institution of the Norwegian Ministry of Health and Care Services, has recommended that there is a need for a strategy for digital security in the healthcare sector [8], and that this strategy should build upon the foundation of the national strategy for digital security [19], due to the sector's own distinct challenge related to technology. Their main sector-specific concerns are related to secure collaboration, secure home care and security in the supply chain. This means that the healthcare sector needs a standardised strategy related to security controls, such as identity and access management (IAM), cryptography, securing medical devices, and standardised security requirements for procurement and supply chain management. The risk report by the National Security Authority (NSM) [24] states that risk related to the supply chain attacks is a key concern, since many organisations have complex supply chains that an attacker can use to infiltrate a less secured trusted partner, provider, or third party, to harm the intended target. This is a real concern for the healthcare sector, which relies and depends on service providers, third-party vendors, and collaboration with other actors [8].

These government reports highlight how technology can improve the healthcare sector, but also mention that technology introduces new vulnerabilities and risks that could affect patient security, which is why information security plays a major role in reducing risk to an acceptable level, and in supporting secure and new innovative healthcare technology. To ensure adequate information security in the healthcare sector the different public organisations need a structured approach to managing their information security controls within and outside their organisational boundaries. Organisations must have a good oversight of their information security posture, to balance risk with information security activities, and must ensure that those information security activities are aligned with organisational objectives.

It is essential that organisations take a structured approach to directing and controlling information security activities within and outside the organisation, to ensure that those activities support organisational objectives. The national strategy for digital security competence [20] emphasises that there is a need to improve information security competence according to societal needs, attracting more research, and a special need for specialist competence to ensure national security. We argue that there is a need for more specialist competence on information security governance, which is a sub-field of information security with a focus on ensuring a structured approach to directing and controlling information security controls. This also means that the creation of adequate skills and competence in information security is fundamental to supporting the national strategies for digitalisation in the healthcare sector and digital security. Without information security governance, organisations do not have oversight of their information security controls and their alignment with organisational objectives. My professional motivation is to support these strategies from the Norwegian government and is aligned with my personal motivation. The main

1. Introduction

goal of this PhD project is to contribute to helping current and future experts gain a better understanding of information security from a business perspective.

This thesis has produced research papers and a textbook to contribute to the enhancement of the field of information security governance, to ensure better governance and management of information security controls in organisations, and indirectly supports the various national strategies for digital security. It is not strictly solely for the healthcare sector, but for every sector, either public or private.

1.2 Problem statement

The national strategy for digital security [19] requires that organisations adopt well-established frameworks, standards or *best practice* in information security governance and management. Today, a variety of frameworks and guidelines exist to establish information security governance and management, e.g. ISO/IEC 27001:2022 - Information security management systems - Requirements ([28]), which is an internationally recognised approach for an Information Security Management System (ISMS) according to which an organisation can be certified. Then, we have the *NIST Cybersecurity Framework* ([30]) which is a well-known and recognised framework published in the USA. In Norway we have *Grunnprinsipper for sikkerhetsstyring* ([23]), *Veileder for sikkerhetsstyring* ([25]) and *Grunnprinsipper for IKT-sikkerhet* ([22]) all developed by the Norwegian security agency (NSM) and freely available.

The healthcare sector in Norway even has an industry standard *Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren* ([6]) which is also freely available. However, a risk report from the Norwegian Directorate of e-health states that 88% of public healthcare institutions have an ISMS, while at the same time 22% of security incidents occur due to a lack of prioritisation of information security work, but only 33% state that security incidents that have occurred were due to a lack of security processes, and one third of all public institutions detect security incidents by accident ([7]). These findings are alarming, and the Directorate of e-health questions how effective an ISMS is in practice. We find it really interesting that this is an issue when there is a clear directive from the government that organisations need to adopt an ISMS, and in view of the wealth of resources on information security governance and management that exist commercially or are freely available.

Our observation is that all frameworks, guidelines and standards are generic and not tailored for any specific organisation. These frameworks often specify *what* needs to be documented or implemented to establish an ISMS. What we see by reading the risk report from the Directorate of e-health ([7]) is that most healthcare institutions have documented an ISMS, but that their ISMS is not a process used to direct and control all security activities in an organisation. Hence, there is a fundamental difference between documenting an ISMS and operationalising it. The main limitations and selling points of these standards are the ability to combine different standards to suit organisational needs, which

is a commonly agreed between researchers to be a good starting point. However, we argue that a functional ISMS needs specialist competence to adapt these standards to organisational differences and objectives, as part of the organisation's overall corporate governance model.

To our surprise, there is not much research on *how* to adapt ISMS to different organisations, and following different standards and combining them will still only specify what to implement and not how to realise the utmost potential of an ISMS. We argue that the purpose of an ISMS is to give the top-level management an oversight of the overall information security activities in an organisation, and with this oversight, the management can use this insight to make well-informed decisions about which activities should be prioritised to achieve organisational objectives. This oversight of the information security activities in an organisation is defined as information security posture (ISP), or *sikkerhetstilstand* in Norwegian, and is embedded in *Grunnprinsipper for sikkerhetsstyring* ([23]), *Veileder for sikkerhetsstyring* ([25]), *Grunnprinsipper for IKT-sikkerhet* ([22]), and security-related law ([13]) stating that ISP should be overseen and monitored in an organisation.

However, these documents do not define what ISP is and how to organise ISMS so as to obtain an oversight of organisational ISP. Surprisingly, as identified in paper: I, there are different interpretations of ISP, the concept of ISP is often discussed at different levels, and there is no research or standard to specify *how* to establish an ISMS with the goal of attaining overall ISP. As pointed out in paper: I there is a consensus that information security governance is not only a technical matter, but also a business matter and a subset of corporate governance, which is also supported by the documents mentioned earlier. However, despite emphasising that security is not just a technological issue, these standards are limited to the information security part and do not elaborate on how to integrate this into corporate governance. The risk report from the Directorate of e-health ([7]) shows a lack of prioritisation of information security work, and we suspect that information security specialists lack knowledge of how to integrate security into a business setting, so that top-level management can understand how information security supports organisational objectives. As stated in paper III, there is limited research on how to apply information security in a business setting, which is crucial for future students and specialists to master in their job roles.

1.3 Research questions

This research aims to address the findings from section 1.2, which has revealed shortcomings in information security governance and management. This insight has been used as a basis to propose new approaches for integrating information security in a business setting, for gaining oversight of the ISP, and for translating information security language into business terms to support decision making.

Basically, the aim of this research is twofold: the first is to elaborate on how to organise an ISMS to get an overview of the ISP and then integrate it with

1. Introduction

ISMS in a way that top-level management understands. These two aspects are needed because focusing solely on the information security part is not enough. Harmonising this with business understanding could help security professionals gain a better understanding of how to communicate information security in a way that the business managers understand, to better support business objectives. Without understanding the ISP, it will be difficult for top-level management to support the ISMS, since they do not understand *what's in it for them*.

To address these issues, the first research question focuses on information security posture (ISP) because there are different interpretations of the term and it is discussed at many levels, for example at technical, specific security control, infrastructure and management levels. Some argue that ISP is solely the status of the security activities and some indirectly discuss that it consists of risk management. We need a standardised definition of ISP to ensure a common understanding, and it is important to adopt a holistic understanding since, based on the literature, it is discussed at different levels. We would like to investigate more of the different perspectives of ISP and answer the following research question:

RQ1: *What is information security posture from a holistic perspective and what should it consist of?*

On the basis of the first research question, we can build upon this fundamental definition and components and extend this further to discuss key principles for how to organise the information security governance program to ensure oversight of ISP. The first research question can also give some hints on the different components that together form a holistic understanding of ISP, and give ideas for how to structure the information security governance program so that information aggregates upwards to the top-level management, and how it can be used to direct and control the program so it can be aligned with organisational objectives. Based on this, we would like to investigate different principles of how to organise an information security governance program to obtain an oversight of ISP and answer the following research question:

RQ2: *How to organise the information security governance program to gain oversight of the information security posture?*

This research question aims at proposing principles and methods to organise information security governance with the goal of achieving oversight of ISP. The first two research questions concern developing a method that could support the organisation, but the final research question is to merge this knowledge, so as to apply the information security management and governance field in a business setting. Based on this, we would like to investigate the business aspects of information security to communicate ISP and answer the following research question:

RQ3: *How should the information security posture be communicated to*

executive management, and used for better decision making?

The goal of answering these research questions is to support existing frameworks, guidelines, standards and strategies regarding information security governance and management. It is important to emphasise that our contributions are not aimed at replacing or contradicting existing contributions, and thereby enhance the field of information security governance. Our contributions could be seen as in-depth guidelines. Our main motivation is to support the existing national strategies in Norway regarding information security. We believe that special competence in information security governance is fundamental and necessary in order to have an oversight of ISP within and outside the organisation, and we hope this research project can inspire more people to conduct further research on this topic.

1.4 Research strategy

The research strategy used to answer the research questions defined in Section 1.3 is provided in Figure 1.1.



Figure 1.1: Research strategy.

To justify our research strategy, we took inspiration from Verne and Bratteteig [33]’s conceptual framework to describe, reflect on and select appropriate research strategies. To develop the most suitable research strategy, we needed to consider the type of research questions we would like to answer, to give us ideas of which research philosophical assumptions are appropriate for this research strategy. Verne and Bratteteig [33] argue that there is no standardised view on the differences in research methodology and methods, and we use their suggestions in our research to discuss the differences. Methodology is our approach to answering a research question, and method is a *recipe* for collecting and analysing data as part of methodology (Verne and Bratteteig, [33]). Both data analysis and collection are described in the research method. However, we also separate them into two different subsections to discuss them in greater depth and provide examples. Then, we will discuss the limitations of this research and end this section by presenting our project timeline. A short summary of the research strategy is provided in Table 1.1.

1. Introduction

| Research strategy | Method |
|----------------------|--|
| Research Questions | Normative; Descriptive |
| Research Paradigm | Interpretive; Pragmatism |
| Research Methodology | Qualitative |
| Research Methods | Grounded Theory; Systematic Literature Review |
| Data Collection | Research Papers; Interview; Textbooks; Industry Papers |
| Data Analysis | Full-Text Assessment; Initial Coding; Core Category; Axial Coding; Constant Comparative Analysis |

Table 1.1: Overview - Research strategy.

1.4.1 Research questions

Holter and Kalleberg ([10]) argue that it is important to reflect on and be aware of the type of research questions we want answered, since the research question can guide us to choose an appropriate research strategy. Based on their argument, they describe three types of research questions; descriptive, normative and constructive. The present study consists of all three types of research questions, but the main type is normative. The reason is that these research questions discuss how actions or circumstances should be, and hence the main trait of the present research is to produce recommendations.

However, RQ1 has elements of a descriptive type of research question because, to give normative recommendations, we need to gain an understanding and description of the current state of research. The main idea of this research is to turn the normative questions into constructive questions, because we want to apply our recommendations in practice, which is the nature of constructive research questions, by making actual changes. However, due to unforeseen circumstances and prioritisation of this PhD project, we will only give recommendations for further research; hence, this research is based mainly on a normative question, but is also descriptive.

1.4.2 Research paradigm

Myers ([16]) states that every research project is based on some philosophical assumptions about how we view the world and how this knowledge can be obtained, hence the research paradigm. These research paradigms guide and influence our research strategy, and it is important that researchers are aware of their grounds of knowledge and the limitations of the chosen research paradigm. The most common classification is threefold: positivist, interpretive, and critical. These research paradigms are philosophically distinct, but Myers ([16]) argues that there is no clear-cut distinction while conducting research.

The underlying philosophical assumptions for the present study are mainly interpretive research but have evolved to the fourth paradigm, pragmatic. Saunders et al. ([21]) argue that the most important aspect is to adopt the method needed to answer the research questions, and some methods may be more appropriate than others. Hence, pragmatism is known as mixed methods by varying different methods and philosophical positions. A similar statement is issued by Feilzer ([36]), saying that pragmatism positioning is an adaptable method that requires extensive knowledge of both quantitative and qualitative research methodologies and different research methods. Morgans ([15]) addresses a common misconception that pragmatism emphasises *what works*, which is not enough; as a researcher, it is important to ask *why* we choose or combine different approaches. This is why in this research strategy section, we carefully justify each method we decide to be appropriate for this research project.

The present research project started with an interview to map the skills that the ten different CISOs recommended. As the research progressed, we identified that there is limited research on the research questions defined in Section 1.3. This means that we needed to generate new theory, but also collect not only research papers, but also industry standards, mainstream books and certification programs adopted by professionals. In pragmatic research, we can combine different research methodologies, methods and types of data to best answer the research questions.

In this way we acknowledge that this is flexible and needs to be open towards the emergence of unexpected data, due to the vast methods of collecting and analysing data from different sources. Feilzer ([36]) argues that a pragmatic researcher needs to commit to uncertainty and acknowledge that knowledge produced through research is relative. Either way, this research is a combination of interpretive and pragmatic, which is a combination that Goldkuhl ([9]) argues is appropriate, but it is important to address how these paradigms support each other.

In this study, we aim to understand the data collected through interpretation, which is an interpretive approach. However, we would also like to use this understanding to construct this knowledge in a way that it is practical and inspire to improve existing frameworks, which is a pragmatic approach. Interpretive is our base paradigm to generate better understanding, while pragmatism functions as a supportive approach to help us gain a better understanding from different methods, with the goal of answering the research questions.

1.4.3 Research methodology

The most common classification of types of research methodology, according to Myers ([16]), is qualitative and quantitative. The aim of qualitative research is to understand and explain research phenomena and work with qualitative data, while quantitative research originates from natural science, to study natural phenomena and work with quantitative data, e.g. surveys, experiments and formal methods. The main research methodology for this research project is a qualitative approach, since our main data derives from interviews, and analysing

1. Introduction

both research papers and industry standards. This requires us to interpret data and results, although we use a hint of a quantitative approach by categorising and generalising different concepts into categories to give us a better understanding of the data to generate new theory.

Our research mainly adopts the interpretive paradigm, but it is important to be aware that interpretive is not a synonym for qualitative research. Klein and Myers ([11]) argue that qualitative research can be undertaken with a positivist, interpretive and critical stance, and our aim here is to gain a better understanding and give recommendations on the basis of qualitative data; hence, this is qualitative research with an interpretive and pragmatic stance.

1.4.4 Research method

A high-level overview of this research method is presented in Figure 1.2, but mainly this research consists of a combination of two research methods: Systematic Literature Review (SLR) and Grounded Theory (GT).

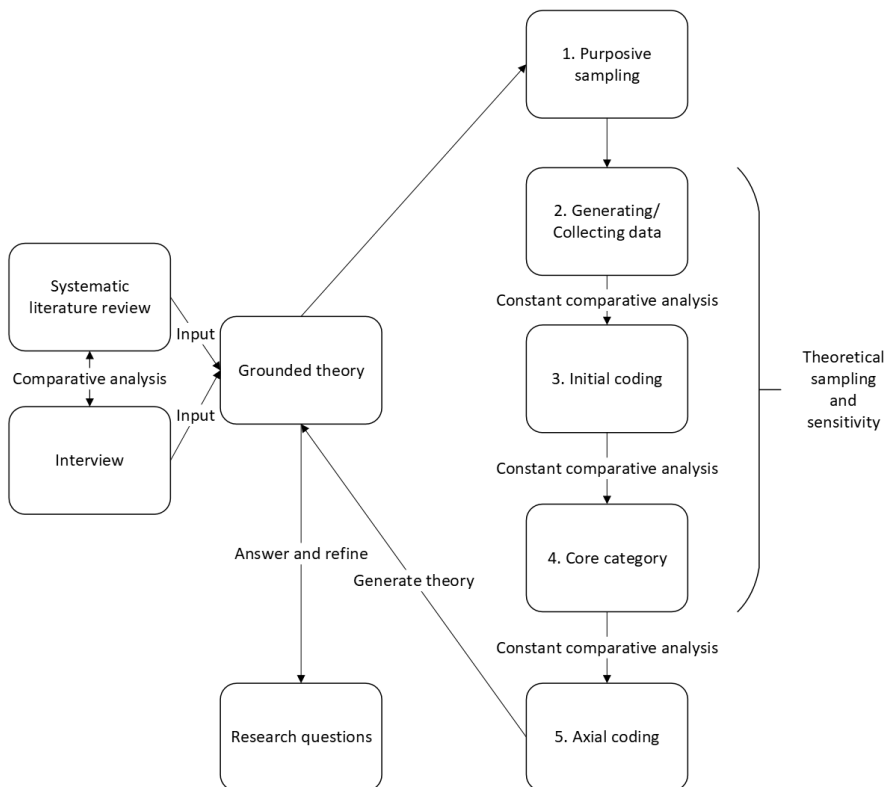


Figure 1.2: Research method used in the project.

The first phase was to conduct interviews with nine current, and one former,

chief information security officers (CISO). The goal in this phase was to collect information about which skills and relevant professional fields are recommended to apply information security management from a holistic approach. We then used a systematic literature review (SLR) to find related research papers about this topic and compared this with the data from the interviews. Surprisingly, we found limited research on the information security governance skills needed to establish a structure to gain an oversight of information security posture (ISP). Having an oversight of ISP is embodied in security-related law and guidelines that our industry must be compliant with. We found limited research-related communication skills, since the CISOs recommended speaking the same language as the business. These aspects were deemed important by the CISOs and discussed in different research papers. As a result, the research questions from Section 1.3 were defined and we chose to use these inputs from SLR and found that Grounded Theory (GT) is the most suitable research method.

This method is appropriate when little is known about a research phenomenon, which is our observation, and our research is to produce and construct new theory. Hence, GT is an inductive approach with the aim of building theory on the basis of gaining an understanding of the research problem first and then making sense of it. The deductive approach involves the development of theory that is subject to a rigorous test to verify or revise the theory, which is not applicable in this project (Saunders, [21]). There are many variations of GT, and the main ones, as described by Birks et al. [2], are classical GT, evolved GT and constructive GT. There are some key differences between them, and we agree with Urquhart and Fernandez [32] that by being loyal to one variation of GT we could be restrictive and not worry about the history of this method. We concluded that the best answer to the research questions is to mix the different principles found in different variations of the method. Hence, we used a modified version of the framework presented by Chun Tie et al. [3], along with the main characteristics and guidelines described by Stol et al. [31] and Birks et al. [2], which is illustrated in Figure 1.2.

The data from SLR and the interviews functions as input for the first phase of GT (described in Figure 1.2), purposive sampling (Chun Tie, et al. [3]). The purpose of this phase is to select relevant data before further analysis. In the second phase, we analyse and re-construct the data to determine whether it can answer the research questions. From phase 2 to 5, this is an iterative process, by conducting constant comparative analysis. As stated by Birks et al. [2], constant comparison is used to analyse data from different standpoints and helps researchers understand their data and the gaps in their data, to generate new theory. By constantly comparing data in each of these phases iteratively, we can use this for coding and categorisation to generate more codes and different categories. Constant comparative analysis helps us to generate, and find differences and consistencies/inconsistencies to help us refine our theories or raise our understanding (Chun Tie, et al. [3]). The constant comparisons help us to collect data based on theoretical sampling, which is to collect data to enrich the emerging theory or concepts until we reach theoretical saturation, when data ceases to give us new insight and we can predict what the analysis

1. Introduction

of the data is likely to describe (Birks, et al. [2]). In a way, this functions as a constantly evolving inclusion and exclusion criterion similar to SLR, but in GT it is called theoretical sensitivity, which is to know what theory is important to our own theory. We used an ever-evolving coding system as an inclusion and exclusion criterion for collecting data until we reached the point of theoretical saturation (Chun Tie et al. [3]).

Although the phase from 2 to 5 is an iterative process, we would like to describe the different coding procedures used in this research project. Stol et al. [31] describe coding as an analytical method to label data according its properties. At the initial coding level, the labels/codes are not categorised, but the main focus is to generate many codes to give us an overview of the collected data. From the initial coding, we can then determine core concepts and use this data to generalise and categorise codes and then transfer the codes to respective categories. The final phase of coding is axial coding, in which the goal is to present interrelated codes or categories and explain the relationships between the data, to gain a better understanding. To analyse and identify the interrelation between the codes and categories, we used a diagramming tool to help us visualise and illustrate the complex interplay between codes (Mills, et al., [14]). The diagramming tool we used was Obsidian, which we used to develop codes, and we then developed categories and transferred the codes to their respective categories. Each code and category was marked and labelled with our interpretations and reconstructed to fit with similar codes. Obsidian can illustrate how the codes are interrelated, and this helped us gain a better overview to generate more theory or collect more data to repeat this research process.

By generating more theory and gaining more understanding, we can use this data to either refine the research question or answer it. To answer the research questions we produced three papers and one textbook. These contributions support and supplement each other and are related to each other in Chapters 2 and 3. All the papers followed a similar approach, since there was limited research on these topics.

1.4.5 Data collection

The three main sources of research data were interviews, research papers and literature from the industry. We only conducted interviews for the paper/book II, while the other papers were based on research papers and literature from the industry. As a starter, to identify appropriate search keywords for literature search, we began with an interview with the different CISOs. Based on these findings, we developed three core categories: Personal development, Management, and Information Security in an information security management and governance context. Then, we identified related codes and transferred them to respective core categories. These core categories and codes function as our inclusion and exclusion criterion for collecting data. This criterion evolved constantly during our research until we reached theoretical saturation.

To collect relevant research papers, we first needed to decide which sources were suitable, and for all the papers, we chose the digital libraries most used by researchers and that covered a wide spectrum of research related to information security. The digital libraries we chose were Web of Science, Scopus and Google Scholar. For all research we needed to choose appropriate search keywords for literature search, and we documented our findings of relevant papers for each research contribution and presented an overview. To find relevant papers, we usually developed inclusion and exclusion criteria or used the core category from GT. We also documented the timeline for each research contribution and used as many iterations of the data collection process as needed, until we reached theoretical saturation.

To develop interview questions, we used the same approach as described for data collection, and we then categorised the findings based on GT into three main topics. Since there was limited research on this topic, I wanted to conduct a semi-structured interview based on the categories, while ensuring that the questions were not too rigid. The questions were open-ended because we wanted to ensure that the subject could explain their approach as much as possible, due to the limited literature. As Crang and Crook ([4]) mention, it is imperative to identify relevant informants for this research first. I had the privilege to have access to my colleagues, who are chief information security officers (CISO) in the Norwegian healthcare sector, and these informants have a minimum of six years' experience with CISO-related work and information security governance and management. Most CISOs also report directly to the steering committee, and I am fortunate to have access to these highly competent colleagues, who can contribute to enriching this research.

I undertook some preparatory work before sending meeting invitations to the CISOs. First, we had a group meeting with all the CISOs in the region, at which I presented that I would be writing a book and proposed that I would like to interview them. The general response was positive, and that they wanted to support my work. Then, I sent a meeting invitation to all of the CISOs, and ten of them accepted the meeting, some of the which were by video. In the meeting invitation, I stated my reason for conducting the interview, and how I would ensure confidentiality verbally when we had the initial talk. I ensured that I had no need to collect personal data and clarified that I would take notes in my notebook with pen and paper (Sikt, [26]). The meeting would be conducted on MS Teams from our company network that has undergone risk assessment and data privacy impact analysis (DPIA), which means that it can be safely used while ensuring privacy.

Walsham ([35]) makes a clear distinction between two types of interview style in the form of passive or overdirection. My main concern was that if I conducted a direct type of interview, the interview subject might not express their views. At the same time, I did not want to be too passive, so that the subject might conclude that I was not interested in their views. The interview style I chose was a balanced approach, which was in-between passivity and over-direction, but also adapted according to different CISOs. The interviews lasted an hour, and some CISOs were eager to discuss more, and since these were my colleagues we

1. Introduction

did not need to *warm up* in case the interview subject was nervous. As stated by Walsham ([34]), that interviews should be supplemented by other forms of data; in our case we supplemented and conducted constant comparison analysis with research papers and literature from the industry.

Since there was limited research on our topic, we needed to collect data from the industry as well and learn how the industry applies information security in a business setting. To select relevant industry literature, we choose the most well-known standards and frameworks, books used as part of the curricula at different universities, and literature from highly regarded certification programs such as CISSP and CISM.

1.4.6 Data analysis

To analyse relevant data from the data collection phase, we used concepts from GT and discussed them in-depth in the research method section. However, we will give some examples of how data was coded and categorised, and interconnections between different categories were identified. An example from the research paper written by Ashenden ([1]) is provided in Figure 1.3.

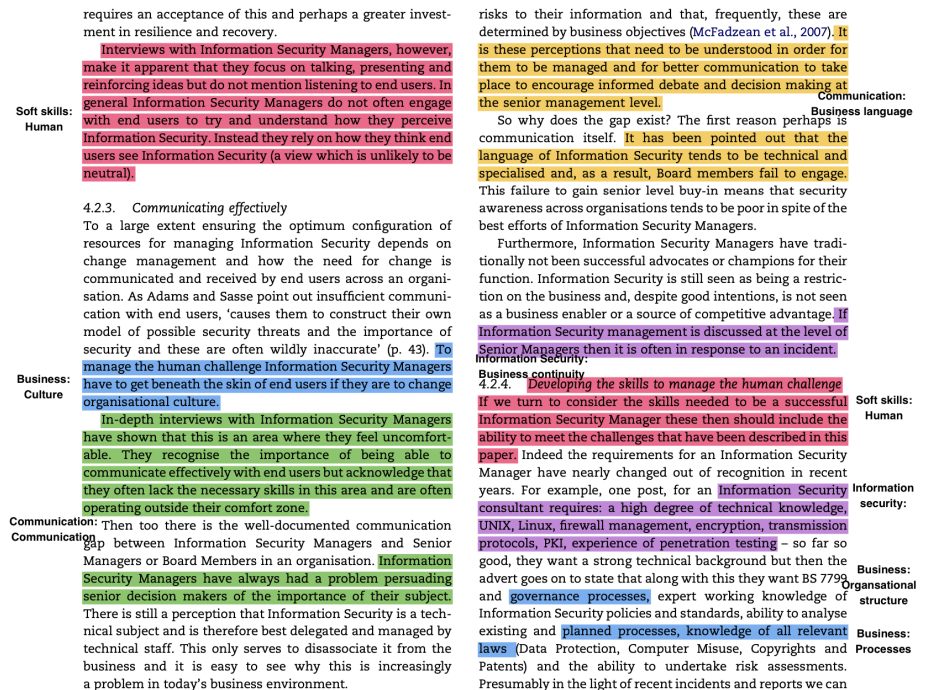


Figure 1.3: Example -Coding.

We started by highlighting relevant phrases, and then we labelled these with colour coding to distinguish between categories. Each of them was labelled with

a category, including the corresponding code. Then, we transferred the codes and categories to Obsidian. This includes the phrase, our analysis of the phrase, and reference to the author. Obsidian is our knowledge base for note-taking and diagramming, to discover connections between different codes and categories. Then, we could use Obsidian to analyse our data and give us an overview of every code, and categorise them to facilitate their constant comparison. An example of a coding table is provided in Table 1.2 from paper III.

| Core Categories | Codes |
|----------------------|---|
| Business | Business Case; Connection; CSF; Culture; Decision-Making; Leaders; Management; Organisational Structure; Processes; RASCI; Risk-Based-Approach; Stakeholders; Top-Management |
| Communication | Business Language; Communication; EAM; Fear Appeal Theory; Likelihood Model; Modelling Language; Persuasive Rhetoric; Reporting; Rhetorical; SBPMN; Solutions; Storytelling; Strong Arguments |
| Information Security | BCP; CISO; IS Goals; ISG; ISM; ISM; ISP; Risk Management; Security Metrics |
| Pedagogy | Business Game; Curriculum; Language Development; Task-Based Learning; Vocabulary-Measuring |
| Soft skills | Cognitive Principles; Human; Awareness; Motivate; Personality characteristic; Personally; Security behaviour; Soft Skills |

Table 1.2: An example of core categories from paper III.

Finally, we could generate a graph with Obsidian to visualise how different codes and categories are connected. While having this overview we can still use constant comparison analysis to form and update new connections that would be difficult to discover without a diagramming tool. A high-level example of diagramming is provided in Figure 1.4 of all codes, categories and references related to paper III. These codes are clickable and can be used to get more information about each code, statements, connections and analysis. By having this knowledge base, we could gain an overview of collected and analysed research data, which made it easy for us to extract relevant data to write research papers.

1.4.7 Limitations

We identified six issues, but the first and main issue is related to positionality. Walsham ([34]) argues that we are biased by our background, knowledge and

1. Introduction

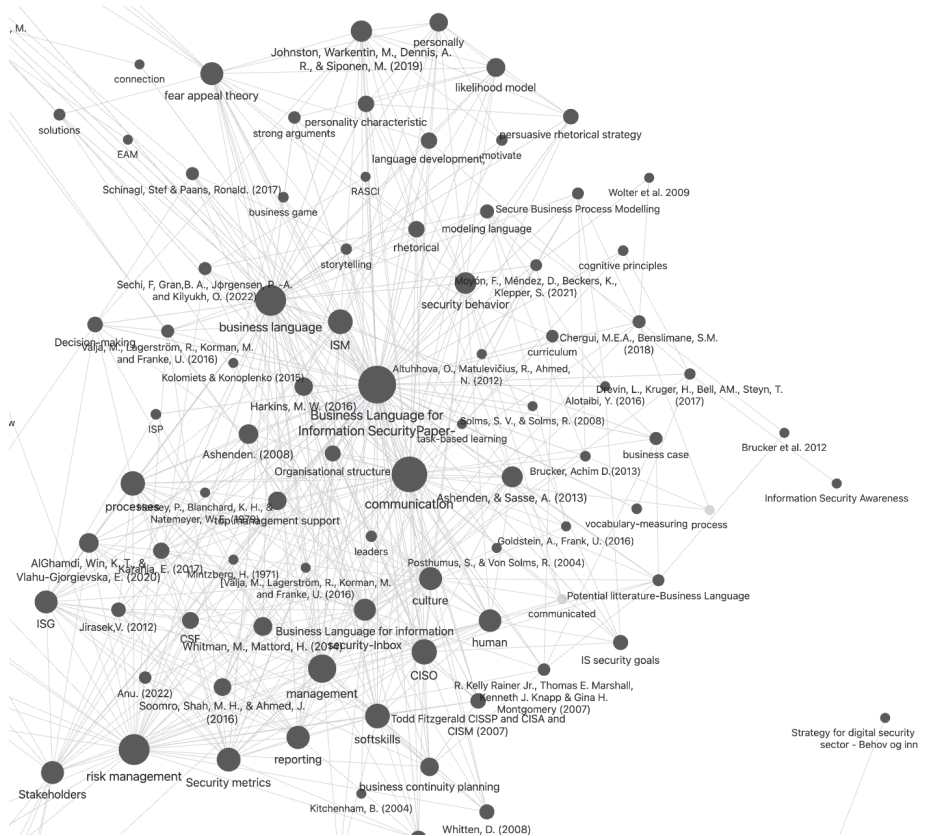


Figure 1.4: Example -Diagramming.

prejudices, which make us perceive differently. Since there is limited research on this topic, it is important to discuss my positionality, because my background and experience in the industry can give predetermined ideas and it is not certain that other researchers conducting the same research process as described in this section would conclude or produce the same results.

For this research, it is important to be aware of the distinction between an outside researcher and an involved researcher (Walsham, [35]). In this particular research, I have adopted an adaptive approach since by interviewing the CISOs I will adopt a more involved style, while on analysing the data I will conduct an outside researcher approach. The main benefit of using the involved approach is a better in-depth understanding of how the health sector works, and the different issues and processes in this industry; however, the limitations could be that these issues are related only to the healthcare sector and are not applicable to other industries. Therefore, I also supplement this research by adopting outside research and collecting research data from others, as well as literature from the industry, to get a better understanding of issues related to information security

governance and management from different viewpoints.

It is important to address that my roles and responsibilities would be less likely to direct the interview answers from the CISOs, since when I conducted the interviews I held the same position as them and I am less experienced as them as CISOs. These CISOs have high integrity and respect in the healthcare sector and would not alter their views and recommendations even if I subconsciously influenced them to give answers to prove my predetermined views.

The second issue is related to validation. The initial plan was to test results from the study in Sykehuspartner Trust by conducting action research to validate and improve our theoretical contributions and frameworks. However, due to unforeseen circumstances and prioritisation, we could not validate the results from this project by conducting action research, which is regrettable, but understandable. Nevertheless, this research has contributed to, and discussed, the gaps in the information security governance and management field, presented different theoretical frameworks to address these gaps, and highlighted the importance of further developing the skills that future specialists need to apply information security in business settings.

The third issue is related to predetermined ideas. Since most of the issues identified are based on my work and practical experience I could already have predetermined ideas or biases that could affect the research results. To address this issue, we applied GT as the main research method to generate a new theory based on the collected data. In GT, some recommend that we should not have any prior experience or investigate relevant literature, since this could contaminate the research, while others take advantage of having experience in the particular field. We adopt the middle position because we would like to be as objective as possible, but also acknowledge that we developed the theory based on our experience. However, our experience is that by applying GT we have expanded our knowledge and understanding, since there were many connections we probably would not have seen had we used another form of research method. Another way to address this issue is to get constructive feedback from a more experienced co-author and discuss our positionality.

The fourth issue is related to generation theory. There is a strong likelihood that another researcher conducting the same research process would get different results, depending on their background. Therefore, my positionality and background from academic and working experience will influence the research in some way. To address this issue, I wanted to first choose the most suitable research process that could reduce my own research bias to an acceptable level, and document each step of the process to hopefully make this research process reproducible. The research process is provided in this section, and we justified that adopting GT as our research method could help us generate theory with inspiration from different viewpoints. To strengthen the generation of theory, we also applied generalisation based on collected data. Lee and Baskerville ([12]) present a framework that organises four different forms of generalisation, and the form applicable to this research project is *Generalising from data to description* because we are generalising empirical statements to generate new statements, and hence generate new theory. This is described earlier by making

1. Introduction

sense of the codes and then transferring them to corresponding categorising, of which examples are provided in Table 1.2. This helped us to make sense of the interrelation between the codes and categorisation, which would not be possible without generalisation.

The fifth issue is related to the possible violation of the Klein and Myers ([11]) principle of multiple interpretations. Because I am interviewing my colleagues from the same sector and have similar work experience, we have the same “language” and perspective on the subject. This could result in only seeing the issue from one perspective, and being blind to the perspectives of people in different industries. To address this issue, we added other research data and literature from the industry to supplement the data from the interviews. Using GT and constant comparison analysis with a focus on generalisation of coding categorisation could help us compare different views and understand them from different perspectives.

The final issue is related to the interpretation of the data from the interviews. Since some meetings were conducted without video and only sound, I could not read body language, so it was difficult to rely solely on verbal aspects. According to Klein and Myers ([11]), this is a violation of the principle of interaction between the researcher and the subject, which states that you get a better understanding of the case by ensuring that you include a method for social interaction between participants and researchers. However, the interview questions were open-ended and developed according to a pre-set checklist of topics to cover. Since the questions were open-ended, the subjects could elaborate on whatever they thought was important. In the meeting invitation, it was stated what the interview topics were, which gave them more time to prepare for the interview. However, since there were open-ended questions, I could miss some key explanations, since I was multitasking between listening and taking notes. To address this issue, I tried to interpret the answers and repeat them, to verify that I understood correctly. There is a possibility that even if I repeated wrongly the subjects would not correct me. However, even such a possibility would not reduce the validity of the collected data, because the results from this research overwhelmingly concluded that there is very limited research on how to apply information security in a business setting by a methodological approach, which is an observation that was further strengthened by the interviews.

1.4.8 PhD research project timeline

I was formally admitted to the PhD programme at UiO in January 2022, but actually started the investigation for the research project six months earlier, based on my own interest. The PhD project timeline is visualised in Figure 1.5, which uses colour labelling for an easier understanding. The green lines indicate when the PhD project officially started and ended. Yellow labels indicate when a paper was submitted, while red labels indicate when a paper was rejected by a conference or journal. Green labels indicate when a paper was accepted, and finally, blue is when a paper was published.

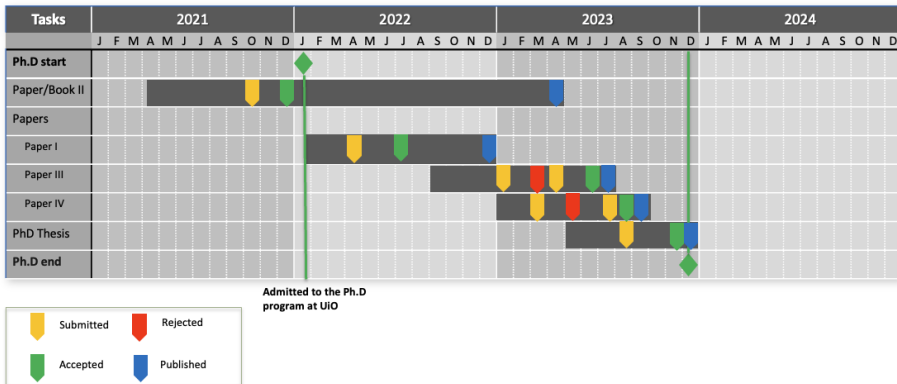


Figure 1.5: Research project timeline.

1.5 Structure of dissertation

This work is written in the form of a cumulative thesis compiling three papers and one book. The thesis consists of four chapters: Introduction, Contributions, Conclusion and Papers. The first chapter starts with an introduction to this research topic, and the underlying motivation and problem statement, and then defines the research question and presents the research strategy for the project. The second chapter starts with a summary of all three papers and one book. The third chapter presents a conclusion and a summary of how all four contributions answer the research questions. The final chapter consists of three papers and one book used for this thesis.

Chapter 2

Contributions

2.1 Summary of papers

Paper I: Information Security Posture to Organize and Communicate the Information Security Governance Program:

This study identified three main issues. First, information security posture (ISP) is interpreted differently at different levels and discussed indirectly with other terms such as oversight, oversee and security status. Second, there is no research or industry standard that provides a framework on how to organise an information security governance program (ISG) to gain an oversight of ISP. Finally, there is limited research on how to communicate the results from the ISG in a way that top-level management can easily understand and act upon.

From the three issues we first argued and proposed the need to define ISP, due to the lack of standardisation, and this term is also embodied in security-related law. We then discussed the existing interpretations of ISP and its limitations. Most defined ISP as the status of information security controls, technological or at a management level. We argue that information security and technology in general are dynamic and that relying on status is not sufficient to make good decisions. We argue that risk, uncertainty and status are the main components of ISP. Risk is used in conjunction with security status to predict and prepare for the ever-changing threat and risk landscape. Uncertainty is an important component of ISP because, as security professionals, we need to address management when proposing assessments based on data from an ISP, when it is important to state the uncertainty levels of the assessment. Because the status of ISP is ever-changing, and information security professionals cannot behave as fortune tellers, it is important to add uncertainty as a component of ISP. Based on our discussion, we proposed a definition for ISP and provided a conceptual model to support the definition.

On the basis of this definition, we proposed to split and define ISP into three different levels: strategic, tactical and operational. From the study we identified that researchers typically discuss ISP at different levels, which is why we propose separating the levels in order to standardise and ensure a common understanding when discussing ISP. The basic definition is the overall ISP, while the definition of ISP levels is to clarify the differences in the levels. These levels are related to how they together describe how to organise ISG to gain an oversight of ISP. Then, this can be applied to direct and control security activities at all ISP levels. This can ensure that top-level management are able to align the different posture levels with business objectives, including the top level. By directing and controlling at all ISP levels, governance can be made more manageable and give

2. Contributions

executive management a holistic oversight of the ISP and ISG program.

Since every organisation is different, while standards and frameworks are generic, we propose adapting a process approach to organise ISG to gain an oversight of ISP. The reason is that not every security control is organised under the security team or department in the organisation, as different security controls and activities can be managed under different groups or departments, such as database, network, operations and human resources. To address this issue, it is necessary to develop guidelines for information security professionals to organise the security controls from a process-oriented approach, since the goal is to remove barriers between functional groups by organising cross-functional teams, which is process management. This study does not present the details of a process-oriented approach, but highlights the importance of developing a process framework for information security and providing ideas for future research.

Finally, we developed two different models to communicate with executive management, and some reporting concepts. First is the posture levels criterion, which can be used at all ISP levels. This means that the process manager for each posture level can assign a posture level based on the average score from the different metrics collected, which determines the conformance level according to individual ISP objectives. The same concept applies when posture levels aggregate up to a higher posture level. This concept can be integrated into a dashboard to monitor and collect measurements, after which the executive management will have an oversight of the organisation's ISP and can use this information to direct and control the ISG program, ensuring alignment with business objectives. The second model is related to uncertainty, and the purpose is to communicate confidence level in posture assessments or reports. This model is used to build an understanding that information security work is clouded with uncertainty, and it is important to have a model that can accommodate and express levels of confidence.

Paper/Book II: Informasjonssikkerhetsledelse - En holistisk tilnærming / Information Security Management a Holistic Approach:

This study began by identifying the skills and subjects recommended to build competence in applying information security management in a practical business setting. The research method for this study is a combination of interviewing ten CISOs, supplemented with SLR and GT. We then applied constant comparison analysis of the data to find that there is not much in-depth research into what skills and fields are needed to adopt an holistic approach to managing information security. Research papers we collected mention mapping and recommend skills and relevant subjects; yet there was limited in-depth research of this topic, which was surprising.

Due to limited research of this topic, I began systematising the research findings and sought to combine this with my own working experience in the industry to write a textbook *Information Security Management - A Holistic Approach..* This book can be seen as an extension of the recommendations from interviews and research literature and in greater depth considers the skills and

subjects recommended to apply information security from a holistic approach.

From the data collection, we categorised the findings into three main components that form a holistic approach to information security management: personal development, management and security technology. Then, we added a fourth and final component to combine these components, since they are related to each other and function as our framework to learn information security management with a holistic approach.

This book starts with personal development and explores the relevant subjects that could help a security professional develop personal skills. A person who works with information security management will collaborate with different people from the organisation, and not only technical or security people. This makes it important to be aware of oneself to develop skills to understand oneself and relate to others. Building personal skills is important to ensure good collaboration and the confidence to present and negotiate with key stakeholders. Building these skills lays the foundation for an understanding that could be used to further develop your management skills and information security management.

The book then transitions to the management part and considers the relevant management subjects in greater depth. The aim of this part is to gain a better understanding of the business aspect of information security and to understand how business people think. Gaining this understanding can help security specialists understand and adapt their security strategies according to business objectives. Another goal is to build a management repertoire to practice management from different levels. I thus defined four levels of management that an information security management specialist should know: interpersonal leadership, management, governance and information security management. Examples of sub-fields are the following: interpersonal leadership focuses on learning strategies to motivate and coach others, where the interviews and literature indicate that conflict management is important, because as security specialists we might meet people who do not agree with our recommendations, since these could require others to change the way they work and increase their workload. Therefore, learning conflict management is essential. Personal development can be seen as an essential requirement for a security manager, since this is transferable to interpersonal leadership and managing conflicts. For example, how can you motivate others if you do not know how to motivate yourself? Even if you know how to motivate certain people, it is still uncertain whether you can motivate other personality types. Building interpersonal skills is the foundation for understanding yourself and others, and forms the basis for understanding and adopting more extensive strategies to motivate other personality types.

The management part focuses on learning strategies to build and understand the organisational structure, to develop and manage processes, and to structure roles and responsibilities between different security specialists. In the data collected it is, for example, stated that it is important to have skills in organising a security department and managing controls, but we could not find any literature on how to learn this from a security perspective. The governance part focuses on learning and understanding corporate governance structure and decision-making

structure, and developing strategies and metrics to support business objectives and decision-making models. The main objective of learning these subjects is that an information security management specialist could integrate ISG into corporate governance and establish a decision-making structure related to security. An information security specialist could be a decision maker, making it important to learn decision-making models to ensure well-informed decision-making.

The book then focuses on relevant information security subjects from an information security management and business perspective. The general idea is that a security management specialist cannot be an expert in everything, and especially not in a field as broad as information security. We categorised information security subjects into three different levels of understanding: basic, intermediate and specialist. The subjects at the specialist level were discussed in-depth, while the other levels were covered at high level, with some exceptions for subjects at the intermediate level. Topics at the specialist level are aligned with management fields such as information security governance, security and risk management, since a security management specialist will integrate security-related work as a natural aspect of an organisation's processes and structure.

All of these three components: personal development, management and security technology, are interconnected and can help a specialist to apply information security holistically. Personal development might, for example, help you to be a better manager, and understanding the management aspect could help you understand how information security can support business objectives. The fourth and last component is how to combine the three components together, where the book provides a model for universal aspects, and shows how these aspects are integrated. To present the universal concept in practice, we provided examples of the similarities of the different subjects. By understanding the similarities it is easier to remember the various elements of the book. As a result, this book presents a method for how information security professionals can learn to speak the same language as business leaders.

Most books and literature focus predominantly on the traditional technology and management aspects of information security, while this book is, to the best of our knowledge, the first to present a model to combine personal development, management and information security to gain a holistic approach to information security management.

Paper III: Business Language for Information Security:

This study clarifies that information security researchers and professionals acknowledge the importance of speaking the same language as the business units in an organisation, to ensure that security is understandable for executive management. If top-level management do not understand how information security can support the business objective, security will not receive appropriate attention and prioritisation. Information security specialists need the skills to translate the information security language into business language. The study identifies two main issues related to this topic. First, even though there is a clear consensus regarding *speaking the same language as management*, the

researcher and the industry used different terms to describe the topic directly or indirectly. We chose to define this topic as *Business Language for Information Security (BLIS)* and provided a definition with the goal of a standardised term to ensure a common understanding, serving as the foundation for developing a method to learn it. Second, there are limited research papers discussing what business language is. Only a few publications discuss what it consists of and none discuss how to learn it. This is quite surprising, given that a large number of papers state the importance of communication, reporting and communicating with top-level management. Even a well-known standard such as ISO/IEC 27001:2022 ([28]) specifies that top-level management must demonstrate leadership and commitment to ISMS, but does not specify how to build up trust and understanding of information security to gain support.

To address the first issue, we proposed a definition and named it *Business Language for Information Security (BLIS)*. The study argues that the purpose of learning BLIS is not simply to speak using the same terms as management, but also to understand the business side of information security. By gaining a better understanding of the business side, the specialist can identify business patterns, such as how corporate governance is structured, in terms of organisational structure, process management and decision-making structure. Then, a specialist can use this knowledge to adapt information security work into an existing organisational structure. By gaining this understanding, a specialist can negotiate with top-level management in a language they understand. Based on our observations, dedication is required to learn business subjects and other relevant subjects integrated with information security. Hence, we argue that BLIS is not just for communicating with management, but should be a proper sub-field of information security, with the goal of applying information security in a business setting.

From our study, we identified some similarities in concepts discussed by researchers regarding BLIS. We began coding, systematising and sorting the findings into different categories and defined them as five components of BLIS: Business, Information Security, Communication, Soft skills and Pedagogy. These components were chosen to serve as a high-level framework to learn BLIS and to provide ideas on how to develop a curriculum. Then, we discussed and argued why these components are needed and added relevant sub-fields for each component. This study does not consider the sub-fields in depth, but discusses them at a high level and provides ideas for further improvement. For example, to identify relevant business subjects, we analysed which information security subjects such as information security governance and risk management, collaborate with top-level management. Based on this we discussed why it is important to understand the business side, and then we proposed that it is important for future specialists to have an understanding of corporate governance and corporate risk management, since information security is a naturally integrated aspect of these subjects.

To identify relevant sub-fields for communication, we analysed relevant papers and categorised them into high-level subjects. An example of a sub-field is process modelling, which is a visual description and communication method that breaks

2. Contributions

down complex information in a way that makes it easier for non-information security specialists to understand. Then, we presented process modelling concepts that could be useful to learn and use, depending on the recipients, such as Business Process Modelling Notation, Unified Model Language, SecureBPMN and Enterprise Architecture Management. Another sub-field for communication is rhetoric, which is the practice of communicating tailor-made messages as a function of different circumstances and recipients with the goal of persuading listeners. Here, we discuss different rhetorical strategies that could be used, and discuss how security experts tend to use *fear-based rhetoric*, and we recommend that future specialists also learn to use *solution-based approach*. We argue that it is important to learn both *fear-based* and *solution-based* approaches and adapt to situations. For example, a solution-based approach is better than negotiating business or strategic plans and long-term planning. Fear-based approaches are more suitable to handle situations that require swift decisions, such as handling security incidents. It is also important to understand that every recipient is different, and it is important to learn different strategies to persuade others.

In rhetoric theory, it is important to learn different personal characteristics to adapt different communication strategies depending on the listeners, which is why learning *soft skills* is essential. Learning soft skills can help a specialist gain a better understanding of themselves and other personal characteristics that can help them use the most appropriate strategies. Working with information security management requires collaboration with other non-security specialists, which is why learning soft skills to build trust and ensure good collaboration is important. Learning soft skills is related to communication, but also interpersonal leadership and all aspects of applying information security in a business setting; we therefore emphasise this as a discrete component of BLIS.

Finally, to identify relevant sub-fields for pedagogy, we analysed relevant papers discussing how to teach information security. We found *business game* to be particularly relevant and something BLIS teachers should apply. The idea is to simulate real-life scenarios of information security in a business setting, to build student experiences. Another relevant method is the linguistic approach to measure the students' understanding of different terms. It is highly relevant to test the students' understanding of business terms. However, we recommend that the students also learn basic pedagogy, because this gives them a foundation to understand how to teach others and how to learn. Without this understanding, it is difficult to gain support from management. The goal is to help management understand information security, not just to *tell* them. It is important to learn how to transmit information simply so that they understand enough to make well-informed decisions. Learning pedagogy is not only for teaching BLIS, but also for understanding how to simply transmit information to other collaborators.

Based on this research, we conclude that BLIS is far too complex to be viewed simply as speaking the language of business, but should be a distinct field within information security. We argue that all students should have a basic understanding of BLIS, while those who specialise in information security management should be experts in BLIS. The goal is to ensure that future generations of information security professionals not only have a better understanding of the

business side, but also apply information security in a business setting. To the best of our knowledge, this research paper is the first to define and propose different components of BLIS and to provide a high-level framework for how to learn it.

Paper IV: An Opportunity-based Approach for Information Security Risk:

This study identifies the fact that there is limited research and literature related to assessing positive risk, even though the new ISO/IEC 27005:2022 ([27]) has expanded the definition of information security risk to include positive risk. It is safe to assume that business leaders should expect that an information security risk analyst can assess positive risk, since ISO31000 ([29]) already incorporated positive risk in 2009. What we find surprising is that there is limited research on positive risk; researchers such as Olsson ([17]) and Rajbhandari ([18]) conclude in their studies that frameworks and methodologies mainly focus on negative risk. Their research was conducted decades ago, and sadly, based on our study, we can confirm that there has been very limited advancement in approaches to positive risk. We identified two main issues. The first issue is related to the new definition of risk from ISO/IEC 27005:2022 ([27]) which is too abstract and impractical to describe both positive and negative risks. The second issue is the lack of a method to assess positive risk.

To address the first issue, we explain the limitations of the definition and supported notes from ISO/IEC 27005:2022 ([27]). One of our main arguments is that the definition is at an abstract level, and only makes sense when an organisation does not apply risk management. We propose to separate the definition into two different levels, one at an abstract level and the other at a professional level, like applying risk management. We recommend using events in the definition, since this is neutral, and both threats and opportunities are a type of event. Then, we propose a professional definition of risk that is open for both positive and negative risk, and then define what we mean by positive risk. We consider that it is not necessary to define negative risk because the definition from ISO/IEC 27005:2022 ([27]) is sufficient.

From the definition we deduce a general risk description template that is aligned with the definition of professional risk. The template accounts for describing both positive and negative risk. This opens up four possible strategies to frame risk, depending on the recipient's risk perceptions. The first alternative is to frame the event as a threat, which, if the event materialised, would result in a loss. The second alternative is that the threat would lead to a gain. In the third alternative, we see the event as an opportunity, which, if materialised, would lead to a loss. The last alternative is that the opportunity leads to a gain. The traditional way of describing and presenting risk is based on alternative 1, but now we have three more options to frame risk depending on the decision-maker's risk perception and personality.

Since this is a new way of thinking for information security risk analysts, we provide a fictitious case with different stakeholders. Then, we propose which alternative is most appropriate for the recipients and include the risk assessment.

2. Contributions

Based on this case, we emphasise that every risk, either positive or negative, needs to be managed. An opportunity to improve a process or acquire a more robust system does not necessarily mean that a gain will result from this opportunity. This depends on how the opportunity is managed; for example, have we employed security controls to increase the likelihood of achieving this opportunity? If the opportunity is actually achieved and the organisations have improved their processes and have a robust system, have we employed security controls to gain from this project? If we do not manage risk, the system could be more robust, but instead the workload has increased for the employees. The aim of this case is to showcase that a risk can be communicated either positively or negatively. For as long as a risk has not yet occurred, this gives us the freedom to frame risk the way we want. In this case, we identify, for example, that a medical system does not have monitoring capabilities; therefore, the goal of this risk assessment is to recommend acquiring monitoring capabilities to reduce workload. We then present four different strategies to describe and communicate risk to different stakeholders either positively or negatively. The aim is to show that we do not always need to emphasise *what can go wrong* when presenting information security risk to stakeholders.

Based on the new definition of information security risk and proposed risk description strategies, we provide concepts and methods to understand and assess positive risk. First, we illustrate and conceptualise our recommendation for defining risk in a way that is easy to understand. Advantages and disadvantages of the traditional definition and our definition of risk are discussed. We argue that risk consists of three components; event, objective and uncertainty. We choose event because we argue that both threats and opportunities are a type of event, while we choose objective because if an event materialises then it affects objective, of which the outcome results in a loss or gain. Event and objective as components both give the opportunity to address the positive and negative aspects of both event and objective, and do not limit to negative risk like other models. In our study we argued that the existing definition of risk can be interpreted as uncertainty affecting the outcomes, and we argue that this could be misunderstood as uncertainty only affecting the outcomes. In our conceptualisation of risk we illustrated that uncertainty affects both the event and objectives/outcomes. The aim of this conceptualisation is to emphasise that uncertainty affects both event and objectives, and not just the latter part. The risk analyst needs to manage uncertainty when assessing the likelihood of the event occurring, and assessing the consequence if the event materialises.

Finally, we propose a risk assessment matrix that is aligned with the risk description strategies that we proposed earlier. Since we have four alternatives to describe and communicate risk, this matrix is a four-dimensional risk matrix. This model is a conceptualisation and can be adjusted depending on organisational differences and risk appetite. However, this model can be used to assess both positive and negative risks, while helping risk analysts reflect on risk from different perspectives and visualising risk for decision makers. To the best of our knowledge, this research paper is the first to elaborate on positive ISRM, proposing strategies to describe and assess both positive and negative risks,

which are aligned with the new information security risk definition from ISO/IEC 27005:2022 ([27]). We conclude that the risk management field is evolving and that information security specialists need to adapt to this change and understand more of the business side, and we hope that this study encourages others to gain a greater understanding of positive risk.

Chapter 3

Conclusion

From the problem statement in Section 1.2, the risk report from the Directorate of e-health ([7]) stated that 88% of public healthcare institutions have an ISMS, but that the lack of prioritisation nevertheless leads to significant risk exposure, with serious security incidents as a consequence. We found these results surprising, especially since management support is a fundamental requirement and the Directorate of e-health questions how effective an ISMS is in practice. This thesis provides enhancements of the information security governance and management field by addressing these issues and underlining the importance of learning the business aspects of information security, since this can help a specialist communicate to the management in a way they understand. In particular, both business and information security are constantly evolving, and professionals in information security need to adapt to this change and expand their knowledge and understanding of the business side and not rely solely on technological expertise. On the other hand, business leaders need to understand how technology and information security can support the business and give a competitive edge over other businesses, which means that information security is not only a technological issue, but also an important business issue.

We argue that to get top-level management's support and ensure that they give information security adequate priority, it is important to understand how business leaders think in their field, but also show them how information security actually supports the business objectives. We argue that this is the missing link, since there is limited research discussing *how* we can achieve these aspects. This project has presented a framework named Business Language for Information Security (BLIS) for this purpose, which is a framework to learn, understand and apply information security in a business setting. This could help top-level management understand how information security can support business objectives. But understanding is only the first part, and to reinforce this the security specialist should show how security actually supports the business objectives. This is why this thesis presents a framework to organise information security governance, to gain an oversight of the information security posture (ISP). We describe a structure to direct and control ISP at the different levels, and show how each posture level conforms according to predetermined baselines. The security specialist can use the posture levels as data to help management understand the current level of ISP. We found that the existing frameworks are generic and limited to the information security perspective. These frameworks only specify what to implement and not how to implement an information security governance program. The contribution from the present study can help security specialists understand how to implement an information security governance program tailor-made for an organisation.

3. Conclusion

Existing frameworks do not usually adopt a holistic view of information security, but focus on negative risks. Information Security Risk Management (ISRM) is an important component of ISG and ISM. Traditional ISRM is limited to threats, which can be summarised as *what can go wrong*, hence negative risk. However, the new ISO 27005:2022 has expanded its definition to include positive risk, while not developing any guidelines on how to conduct positive risk assessment. Based on this issue, we have expanded the definition of risk and made it more applicable in an ISRM context. We have also proposed strategies to describe risk in four different ways, depending on the risk perception of the decision makers. Then, a four-dimensional risk matrix was developed for assessing both positive and negative risks. These contributions have also supported a holistic understanding of ISP, since ISRM is a core component, and have also developed strategies to communicate risk in simple matters tailored for different decision makers.

It is our hope that this thesis will contribute to the enhancement of the ISG and ISM fields. This thesis has also resulted in a textbook that could be used to teach the business aspect of information security. This represents a contribution to professionalise the information security field and develop a more business-oriented approach. The business and technological environment is constantly evolving, and we hope that these contributions will help information security students and professionals adapt to these changes and broaden their view of information security.

The rest of the chapter summarises how the present study has answered the research questions defined in Section 1.3 and discusses the connections between the contributions, which are illustrated in Figure 3.1.

3.1 Summary of contributions

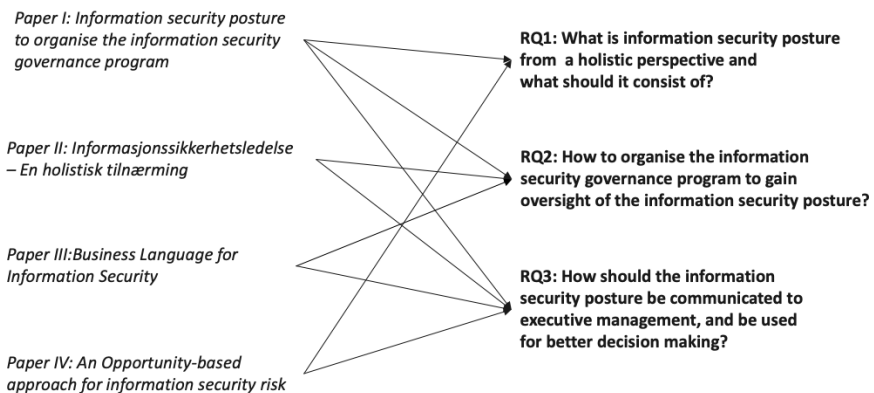


Figure 3.1: Summary of contributions.

3.1.1 RQ1: What is information security posture from a holistic perspective and what should it consist of?

Paper I identified that there is no uniform standardisation of the term ISP. Most research and industry literature discusses that ISP is the status and our observation is that it was discussed at different levels. Paper I discussed and proposed a new definition, and we developed a conceptualisation design of ISP that defined three main components of ISP: status, risk and uncertainty that together form a holistic view of ISP.

Paper IV further extends the results from paper I. This study identified that information security risk emphasises threats and negative risk, while positive risk is *forgotten*, even though the new ISO/IEC 27005 ([27]) has incorporated positive risk. However, there is limited research on positive risk, and we developed methods to identify, describe, assess and communicate positive risk. This contribution has expanded the holistic view of ISP to add positive risk.

3.1.2 RQ2: How to organise the information security governance program and gain oversight over the information security posture?

Paper I discussed that frameworks, guidelines and standards usually specify *what* to implement, but not *how* and *why*, and identified an issue related to the fact that security controls can be managed by departments other than the security department. A recommendation to address this issue was to implement a process management approach to remove boundaries and support cross-functional teams, but this study did not elaborate on how to actually establish processes to organise an information security governance program.

Paper/Book II extends previous work done in paper I by writing a textbook that gives readers a better understanding of the business aspect of information security. This book presents relevant knowledge that can be used to understand how an organisation is structured and how to use this understanding to organise the information security governance program accordingly. Some examples of the relevant management field presented in this book include corporate governance, process management, organisational structure, and developing roles and responsibilities, and many more. In short, this book provides a specialist with the knowledge they could use to organise an information security governance program.

Paper III identified that there is a consensus among researchers that information security governance should be a natural aspect of corporate governance. This could indicate that security specialists should have a basic knowledge of corporate governance. Some researchers discuss the importance of having knowledge of organisational structure to facilitate effective workflow, and other researchers argue that establishing cross-functional teams is important, since information security is ingrained in most business processes. This could indicate that process management skills are important to support these statements. In this paper, we presented a framework to learn Business Language

3. Conclusion

for Information Security (BLIS) that can be used to understand more of the business side and to apply information security in a business setting. This paper argues that having knowledge in business fields such as process management and organisational structure is important to organise an information security governance program. However, this paper does not elaborate on these topics in depth, but the paper/book II can be seen as an extension of this paper and goes into more detail.

3.1.3 RQ3: How should the information security posture be communicated to executive management, and be used for better decision making?

Paper I discussed that frameworks, guidelines and standards on what to implement, and how these standards specify controls related to security reporting, is important to obtain management commitment and support. However, these standards do not specify how to actually communicate in a simple manner that the executive management understands. Based on this issue, this paper proposes two models: posture-level criteria and uncertainty level. Posture-level criteria can be used to report the level of conformance of ISP in an easy-to-understand matter and can be integrated into a dashboard. The uncertainty level is used to assess the uncertainty of reported ISP levels, to ensure that uncertainty is managed to an acceptable level, and to ensure that top-level management does not take decisions on highly uncertain ISP assessments.

Paper III goes into more detail by proposing a high-level framework on how to learn the Business Language for Information Security (BLIS) and proposes five components that a specialist should have knowledge of: Business, Information Security, Communication, Soft skills and Pedagogy. Each of these components was discussed based on existing research and resulted in recommendations for which sub-fields of each component a specialist should know. By learning BLIS, a specialist can understand the business field and use this knowledge to their advantage, such as translating information security language into business language. However, this paper does not go into greater depth concerning the sub-fields of the components.

Paper/Book II extends the contributions from paper III and considers sub-fields of the BLIS components in more detail. However, this study takes it even further by presenting a method to learn BLIS, and since this is a textbook it can be used to teach future students how to apply information security in a business setting.

Paper IV supports previous contributions by presenting different strategies to communicate and describe risk in both positive and negative ways. One of the main findings from this study is that information security tends to use a *fear-based approach* to present risk, but this study encourages future specialists to frame risk in a positive way, or from a *solution-based approach*. The general idea is to frame risk according to a decision maker's risk perception, which means that if a decision maker prefers a solution, the risk is framed according

to a *solution-based approach*. This means that learning to view risk from both a positive and negative perspective opens up more ways to communicate risk, depending on the recipient's risk perceptions.

3.2 Future work

The purpose of this research was to adopt the new theoretical contribution and conduct action research to validate the research data. The plan was to improve the information security governance program in Sykehuspartner, with the aim of attaining an overall ISP. Sykehuspartner is the largest healthcare provider in the Nordics, with a complex organisational structure, which makes it the ideal company to test and validate the robustness of new theoretical contributions. Unfortunately, due to unforeseen circumstances and prioritisation, we could not validate the research data in this project.

However, in future work, we will validate the contributions of this research project, and even though these contributions are theoretical, they still enhance the field with new knowledge, methods and principles, but also shed light on the importance of gaining specialist competence in ISG and how to communicate the program to non-information security specialists. Hence, as a future research activity we consider the validation of the contributions from paper: III, which is to develop the Business Language for Information Security (BLIS) sub-field within information security, with the goal of practical use of information security in a business setting. Nevertheless we did test some concepts, such as adopting a *business game* approach whereby the students as exercises receive real cases that the lecturer has experienced. This *business game* approach with topics related to BLIS was well-received by students; these results from the students were unintentional, but were a result of course evaluation in which the students could describe in free text what they liked about the course.

Even so, these results were unintentional and show that students could enjoy solving real life or business scenarios. This shows that the contributions from this research project are quite promising and can motivate students to learn more, but also expand the content of teaching for the better. Since we now have a textbook that will be used to teach BLIS, we will try to add more content on relevant existing courses and adjust the teaching content to be more business-oriented. Then, we could test students who have learned BLIS and those who have learned traditional information security governance, information security management and risk management to solve real business cases, to validate whether BLIS has helped the students, or how we can improve the teaching content.

Another way to validate research data is to design a master's thesis that touches upon this subject, and the University of Oslo has many collaboration partners with different organisations in various sectors and industries. This could give the student the opportunity to test and validate these concepts in real business settings, but another benefit is that the student might be even more motivated since they would be working for a company, which could give them subsequent employment opportunities.

3. Conclusion

This research has contributed to showing and underlining that information security is an important part of an organisation, and it is important that security specialists are also familiar with the business side of information security.

Bibliography

- [1] Ashenden, D. “Information Security management: A human challenge?” In: *Information security technical report* vol. 13, no. 4 (2008), pp. 195–201.
- [2] Birks, D. F. et al. “Grounded theory method in information systems research: its nature, diversity and opportunities”. In: *European Journal of Information Systems* vol. 22, no. 1 (2013), pp. 1–8.
- [3] Chun Tie, Y., Birks, M., and Francis, K. “Grounded theory research: A design framework for novice researchers”. In: *SAGE open medicine* vol. 7 (2019), p. 2050312118822927.
- [4] Crang, M., Cook, I., et al. *Doing ethnographies*. Sage, 2007.
- [5] e-helse, D. for. *Nasjonale E-helsestrategi*. 2023.
- [6] e-helse, D. for. *Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren versjon:6.1*. 2020.
- [7] e-helse, D. for. *Overordnet risiko- og sårbarhetsvurdering for IKT i helse- og omsorgssektoren*. 2019.
- [8] e-helse, D. for. *Strategi for digital sikkerhet i helse- og omsorgssektoren - Vurdering av behov og innretning*. 2020.
- [9] Goldkuhl, G. “Pragmatism vs interpretivism in qualitative information systems research”. In: *European journal of information systems* vol. 21 (2012), pp. 135–146.
- [10] Holter, H. and Kalleberg, R. “Kvalitative metoder i samfunnsforskning”. In: (*No Title*) (1996).
- [11] Klein, H. K. and Myers, M. D. “A set of principles for conducting and evaluating interpretive field studies in information systems”. In: *MIS quarterly* (1999), pp. 67–93.
- [12] Lee, A. S. and Baskerville, R. L. “Generalizing generalizability in information systems research”. In: *Information systems research* vol. 14, no. 3 (2003), pp. 221–243.
- [13] Lovdata. *Lov om nasjonal sikkerhet (sikkerhetsloven)*. 2022.
- [14] Mills, J., Bonner, A., and Francis, K. “The development of constructivist grounded theory”. In: *International journal of qualitative methods* vol. 5, no. 1 (2006), pp. 25–35.
- [15] Morgan, D. L. “Pragmatism as a paradigm for social research”. In: *Qualitative inquiry* vol. 20, no. 8 (2014), pp. 1045–1053.
- [16] Myers, M. D. “Qualitative research in business & management.” In: (2009).

- [17] Olsson, R. “In search of opportunity management: Is the risk management process enough?” In: *International journal of project management* vol. 25, no. 8 (2007), pp. 745–752.
- [18] Rajbhandari, L. “Consideration of opportunity and human factor: required paradigm shift for information security risk management”. In: *2013 European Intelligence and Security Informatics Conference*. IEEE. 2013, pp. 147–150.
- [19] Regjeringen. *Nasjonal strategi for digital sikkerhet*. 2019.
- [20] Regjeringen. *Nasjonal strategi for digital sikkerhetskompetanse*. 2019.
- [21] Saunders, M., Lewis, P., and Thornhill, A. “Research methods for business students”. In: *Essex: Prentice Hall: Financial Times* (2003).
- [22] sikkerhetsmyndighet, N. *Grunnprinsipper for IKT-sikkerhet version:2.0*. 2020.
- [23] sikkerhetsmyndighet, N. *Grunnprinsipper for sikkerhetsstyring version:1*. 2020.
- [24] sikkerhetsmyndighet, N. *Risiko 2023*. 2023.
- [25] sikkerhetsmyndighet, N. *Veileder for sikkerhetsstyring version:1*. 2020.
- [26] Sikt. *Gjennomføre et prosjekt uten å behandle personopplysninger*. URL: <https://sikt.no/gjennomfore-et-prosjekt-uten-behandle-personopplysninger>. (accessed: 09.05.2023).
- [27] Standardization, I. O. F. *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*. 2022.
- [28] Standardization, I. O. F. *ISO/IEC 27001:22 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. 2022.
- [29] Standardization, I. O. F. *Risk management — Guidelines*. 2018.
- [30] Standards, T. N. I. of and (NIST), T. *Cybersecurity Framework Version 1.1*. 2018.
- [31] Stol, K.-J., Ralph, P., and Fitzgerald, B. “Grounded theory in software engineering research: a critical review and guidelines”. In: *Proceedings of the 38th International conference on software engineering*. 2016, pp. 120–131.
- [32] Urquhart, C. and Fernández, W. “Using grounded theory method in information systems: The researcher as blank slate and other myths”. In: *Journal of Information Technology* vol. 28 (2013), pp. 224–236.
- [33] Verne, G. and Bratteteig, T. “Inquiry when doing research and design: Wearing two hats.” In: *IxD&A* vol. 38 (2018), pp. 89–106.
- [34] Walsham, G. “Doing interpretive research”. In: *European journal of information systems* vol. 15, no. 3 (2006), pp. 320–330.

- [35] Walsham, G. “Interpretive case studies in IS research: nature and method”. In: *European Journal of information systems* vol. 4, no. 2 (1995), pp. 74–81.
- [36] Yvonne Feilzer, M. “Doing mixed methods research pragmatically: Implications for the rediscovery of pragmatism as a research paradigm”. In: *Journal of mixed methods research* vol. 4, no. 1 (2010), pp. 6–16.

Papers

Paper I

Information Security Posture to Organize and Communicate the Information Security Governance Program

Tran, Dinh Uy, Jøsang, Audun

Published in 18th European Conference on Management Leadership and
Governance

Information Security Posture to Organize and Communicate the Information Security Governance Program

Dinh Uy Tran (<https://orcid.org/0000-0001-5691-7641>),

Audun Jøsang (<https://orcid.org/0000-0001-6337-2264>)

University of Oslo, Oslo, Norway

dinhut@ifi.uio.no

josang@ifi.uio.no

Abstract: Information security practice has evolved greatly from being mostly a technical concern to also becoming a concern of executive management. As a result, there are many different frameworks, guidelines and certification programs for information security governance (ISG) and management. The purpose of these standards and certification programs is to help an organization develop a structured approach for governing and managing information security. However, these standards and guidelines are generic and not tailored for any specific organization. These frameworks usually specify “*what*” should be implemented but not “*how*”. Additionally, these frameworks do not specify “*how*” to communicate the information security posture (ISP) to the executive management in a simplistic manner. This paper first defines and conceptualizes the term *information security posture*, and then proposes a framework on “*how*” to communicate and organize the ISP. Our contribution complements ISG programs adopted by organizations to give executive management a better understanding and oversight. We argue that describing the ISP of an organization will support well-informed decision-making while ensuring alignment with business objectives.

Keywords: Information Security Posture; Information Security Governance; Information Security Management; Information Security Reporting; Risk Management; Information Security Program

1. Introduction

Information security is a topic that receives increasing interest from top-level management. The reason why information security risk has evolved from being mostly a technical concern to becoming a priority for management is that an information security breach could have dire consequences for an organization. It is necessary that ISG (Information Security Governance) is structured in a way that gives an organization oversight over its ISP (Information Security Posture), because this understanding is essential to ensure alignment with business objectives. The term ISP is widely used in the literature but is often interpreted inconsistently because of the lack of standardization. Based on these identified issues this paper discusses three research questions (RQ), as described in table 1:

| | | |
|--|--|---|
| RQ1: <i>What is information security posture from a holistic perspective and what should it consist of?</i> | RQ2: <i>How to organize the information security governance program and improve the information security posture?</i> | RQ3: <i>How should the information security posture be communicated to executive management, and be used for better decision-making?</i> |
|--|--|---|

Table 1. Research questions

It is necessary to get a better understanding of how we want to understand ISP before investigating how it can be leveraged. After achieving an understanding of what it should be by making the term more meaningful and useful, then it is possible to describe more in detail what components it should consist of. On this basis it will be possible to explain, organize and communicate what ISP is, and how to improve the posture.

This paper is structured as follows. The theoretical background which gives an introduction to this topic is described first. Next, we describe how the collected research papers were analyzed and compared. Then, the results of our findings are presented. Finally, the paper ends with a discussion on limitations, suggestions for future research and concluding remarks.

2. Background

The purpose of this section is to give a brief description of ISG and ISP.

2.1 Information Security Governance

There are several different interpretations of what ISG is, but they typically have some core similarities. The common agreement among researchers is that ISG should not be seen as a technical matter, but rather as a business matter and a subset of corporate governance (Soomro *et al.*, 2016; Von Solms & Von Solms, 2006; Pérez-González *et al.*, 2019; Posthumus & Von Solms, 2004). This underlines the importance of implementing a holistic ISG program that includes human, process, physical and technical issues. In addition to the above-mentioned elements, Slayton (2021) expresses the importance of establishing a “chain of trust” in supply chain management. This is challenging, since ISG must then cross the boundary of “internal control”, and be extended to strategic partners.

The purpose of ISG is for executive management to direct and control information security activities in alignment with business objectives (Posthumus & Von Solms, 2004). This means that executive management needs oversight over the ISG program and must monitor and validate that information security controls are performing according to business objectives (Whitman & Mattord, 2014). Validation is based on collecting measurements and metrics to evaluate the overall effect of the ISG program. Anu (2021) states that developing metrics will help organizational leaders to understand the ISP resulting from the implemented controls and support effective decision-making.

When executive management has obtained oversight and understanding based on knowledge, then according to Slayton (2021), it is possible to direct and manage risk by turning uncertainty into known risk, which in turn forms the basis for selecting information security controls to address and modify the business risk to an acceptable level. It is important to acknowledge that the ISP is not a steady state and that the threat landscape is constantly changing (Williams, 2012). Slayton (2021) argues that the increasing complexity and rapid change in technology result in unpredictability and uncertainty when directing the business, even when an ISG program is implemented. An example of complexity is when an organization has interdependencies with other organizations/suppliers. Broadening the scope of the ISG program to address business partners can help an organization turn uncertainty into a known risk and also make an organization more resilient against unknown risk. This means that the ISG program needs to be flexible to incorporate dynamic changes in the environment (Soomro *et al.*, 2016).

The importance of ISG has led to the development of various standards that can be used for certification to attest an organization’s commitment to secure its business (Siponen & Willison, 2009). These standards are developed as the consensus of experts in the field of ISG and management. Based on this, Von Solms & Von Solms (2004) argue that it is unnecessary to spend the effort to “re-invent the wheel” when an organization can “follow a best practice”. There are some limitations to Von Solms & Von Solms (2004)’s statement. As an example, Siponen & Willison (2009) argue that there is no evidence behind the claim that there always exists a “best practice”. Methods of best practice are not consistently published, and hence there is no evidence of the availability of “best practice”. These standards are also generic and not tailor-made according to organizational differences, a fact that conforms to the research of AlGhamdi *et al.* (2020) who concluded that most proposed frameworks are not validated and do not provide any detailed description of how to implement a framework. Even so, there seems to be a common agreement that applying a standard is a good starting point for ISG, and then supplementing with other standards and frameworks to suit the organization (Veiga & Eloff, 2007; Siponen & Willison, 2009; Culot *et al.*, 2021; AlGhamdi *et al.*, 2020).

2.2 Information security posture

As mentioned earlier the purpose of ISG is to give executive management oversight over the organization's ISG program and risk environment. This can be achieved by monitoring the ISP. Whitman & Mattord (2014) and Veiga & Eloff (2007) use the term oversight/oversee, while Young (2008), Johnston & Hale (2009) and Anu (2021) use the term ISP, but we argue that they should be interpreted as being equivalent. While the terms can be discussed at different management levels, it can be argued that for the communicational purpose it is beneficial to standardize and use the term ISP instead of oversight/overseeing the ISG program. The reason for preferring to use the term ISP is that it gives management an indication of what is discussed instead of being something they should oversee. Both Johnston & Hale (2009) and Anu (2021) argue that by monitoring ISP, an organization can indicate the alignment of business objectives, but neither defined what ISP should be. Williams (2012) has defined ISP as an indication of the countermeasures against threats implemented to protect the organization’s resources, while Young (2008) gives a similar definition, which states that it is the current organizational state in activities, interaction and integration of information security objectives. Young (2008)’s definition is also compliant with NIST (2022), which defines ISP as the security status of an enterprise’s networks, information,

and systems based on information security resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes.

The resemblance between the definitions is related to the current state/status of the information security controls, and hence it could be argued that it should instead be called information security status. NIST (2022) has defined ISP as synonymous with security status. However, the literature does not discuss how to assess the ISP or how the aggregation of measurement data flows. Based on these definitions, we attempt to add more meaning to the term and supplement the contribution proposed by Young (2008), Williams (2012) and NIST (2022).

3. Method

This research method is based on Kitchenham (2004)'s procedure for Systematic Literature Review and is supplemented with coding concepts from the Grounded Theory (Mills *et al.*, 2006). This research has been conducted according to figure 1 and is further explained below.



Figure 1. Research method

The research topic was identified based on our own work experience and as the main motivating factor. Two types of search engines were used, here defined as “primary” and “secondary” search engines. The primary search engine is for collecting relevant research papers, which constitute our preferred source. The secondary search engine is for collecting non-research papers, for instance relevant frameworks, guidelines and “best practices” which are supplementary data.

The primary search engine is Google scholar, while ORIA was used to collect relevant research papers, which is a library software from the University of Oslo. The search strings that were used in the preliminary search were: “Information security posture” with 16 400 hits, “Cyber security posture” with 4820 hits, “Security posture” with 5960 hits, “Information Security Governance” with 17 800 hits, “Cyber Security Governance” with 16 200 hits, “Information Security Management” with 42 600 hits, “Information Security Management System” with 25 700 hits and “Information Security Reporting” with 27 600 hits.

The Secondary search engine consists of ISO, NIST, NSA, ISC² and ISACA, which are well known for certifications and developing standards. The search strings were only “information security posture” because they mostly provide standards and material on information security governance and management, but not research papers: The findings are ISO (2 hits), NIST (1079669 hits, but without the ability to filter), NSA (40 hits), ISC² (1 hit) and ISACA (61 hits). Non-relevant papers were excluded from this research based on the title, abstract and keyword in the preliminary search.

The preliminary search phase covers all search strings mentioned above except for “posture” on research papers published in 2021 and 2022. The main reason is that we wanted the most up-to-date research because there are many papers on ISG and management. Then we reviewed the reference list from these papers to identify more relevant papers. “Posture”-related strings were searched with “any time” and the findings were sorted from newest papers to older ones. We used a broad timespan on “posture” because there is less research literature in this area, and we wanted to ensure we could find all relevant papers. The result was that 17 research papers and 1 journal/article from secondary search engine were deemed relevant by reading the title and abstract. We developed inclusion-exclusion criteria (provided in Table 2) to assess the quality and relevancy.

| Inclusion | Exclusion |
|--|---|
| Papers that define Information security posture | Papers unrelated to our research topic |
| Papers that indirectly explain or define information security posture | Papers that contain search strings but do not explain the terms |
| Papers that explain the characteristics of information security governance | Papers that are not in English |
| Papers describing a framework for information security governance | |

Table 2. Inclusion-exclusion criteria

The inclusion-exclusion criteria were applied, and the final list consist of 6 relevant papers. To extract data, we populated a form containing extracted relevant quotes and explanations from different papers. Then we used a concept from the Grounded Theory research method, which consists of developing codes or key concepts from extracted data used for theoretical analysis and identifying core categories (Mills *et al.*, 2006). Then, we could use the codes to discover, compare and correlate with different categories. We used this concept to get a better overview of the surveyed research. We defined 10 core categories with corresponding codes and noted which and how many of the research papers discussed those categories. Some codes are identical or similar in different categories and the logic is to make it easier for us to discover interconnections between different categories even though they are discussed directly/indirectly by different papers.

By reviewing the reference list and data extracted from relevant research papers we identified additional 17 research papers relevant for this research and did another iteration, which identified 11 more papers. After verification of the relevancy, we ended up with 16 research papers and 1 journal article related to ISG, management and ISP. Finally, all relevant papers are listed in the bibliography.

4. Results

This section describes the results from analyzing data extracted from the systematic literature review and presents answers to the three research questions.

4.1 RQ1 - What is Information Security Posture from a holistic perspective and what should it consist of?

The first aspect that needs to be discussed is whether ISP should be defined as just the status of the information security activities in an organization. Both Young (2008) and NIST (2022) state that it is the status, but Williams (2012) does not use the term status but an “indication” of implemented security controls. By using the term indication it could be interpreted as saying that there is still uncertainty and that there are unknown aspects of the implemented controls, a view also supported by Slayton (2021). There seems to be a consensus that ISP consists of the status of the implemented security controls. We argue that both status and uncertainty must be addressed as components of ISP. The difference between a posture and status is that a posture is more dynamic, while status is more static. Information security is as Williams (2012) argues not a steady state because of the evolving threat and risk landscape. Simply understanding the current state is not enough to have a holistic understanding of ISP. We argue that organizations also need the component of being able to prepare for ever-changing threats and risk landscapes to reach a “potential future state”. By adding this component to the definition, then it can address both known unknowns and unknown risks. Without this component then ISP is limited to known knowledge, which simply could be defined as status.

It can be argued that the basis of ISP is the combination of “current state”, “uncertainty” and “potential future state”. Even so, there is an intersection between “potential future state” and “current state” because these components depend on each other in the sense that preparing for the future state needs the understanding of the current state of implemented security controls. By including uncertainty is to acknowledge unpredictability that arises with regard to risk. It must also be communicated to executive management that ISP is dynamic because of the rapid change in the threat and risk environment.

Based on the discussed definitions from Young (2008), Williams (2012) and NIST (2022) it can be argued that their definitions give different perspectives on the ISP. For instance, the definition from NIST (2022) starts with the status of the organization’s network and information systems which clearly is seen from a technical perspective. Williams’ (2012) definition focuses more on the infrastructure security posture and Young’s (2008) view is that ISP consists of controls related to recovery, deterrence, detection and prevention. It can be argued that all of these perspectives are correct because they are discussed at different management levels.

Management levels can indicate a reporting structure and how measurement data aggregates. The meta-study by AlGhamdi *et al.* (2020) shows that reporting is a critical success factor for good ISG practice, e.g. because it improves decision-making. Among the 14 studies that were evaluated by AlGhamdi *et al.* (2020), 2 studies had been validated and the remaining studies suggested the importance of reporting based on prominent frameworks or their own research. Even so, the 2 validated studies did not specify the quality of the validation process.

Even if there is little-validated evidence that a reporting structure is a critical success factor, it is obviously needed so that executive management can have oversight over the ISP. Based on our findings from Young (2008), Williams (2012) and NIST (2022) who discuss ISP at different levels, and from AlGhamdi *et al.* (2020) who discussed the importance of reporting, it can be argued that there are different posture levels depending on the ISG program, which in combination underlines a reporting structure. This is why we propose that the definition should include different levels of ISP that in total give the executive management a holistic oversight. Based on the discussion above, we define the overall ISP as follows:

“The information security posture is the current and predicted future state of information security based on a structure for continuous monitoring and oversight over the current state of an organization’s security controls (organizational, technological and physical controls) and the constantly changing risk environment for predicting the potential future state. The purpose of continuously monitoring and evaluating the information security posture is to be informed about the information security status with related uncertainties, to understand how well it currently supports business objectives and how it can be adjusted to better support business objectives in a changing threat landscape and business environment. The information security posture is conceptualized and illustrated in figure 2.

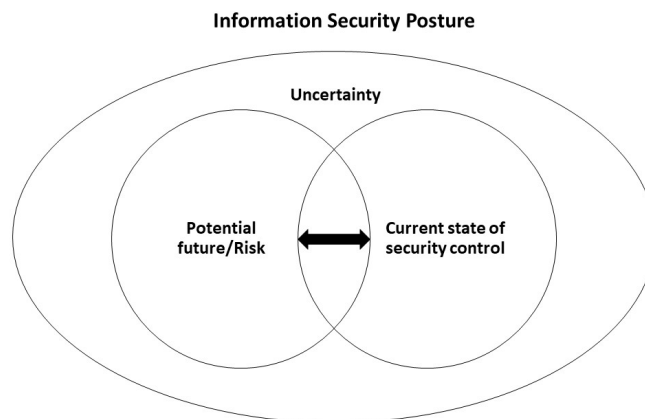


Figure 2. Conceptualization of Information Security Posture

4.2 RQ2 – How to organize the information security governance program and improve the information security posture?

The papers mentioned earlier state that reporting is a critical success factor, but none of them specify “how” to organize a reporting structure. We therefore propose a concept, which is adaptable to different organizations. We also break down the concept of ISP into separate levels, to make it more manageable for instance to conduct a capability maturity assessment on different levels of ISP, which in turn determines the overall ISP.

The main difference between ISP and the maturity level of information security management is that ISP also addresses the degree of alignment with business objectives. Improving the maturity level does not necessarily lead to an improved posture level, since a mature security control/process might not be well aligned with business objectives. Hence, maturity assessment is one of the many tools used to improve ISP. Since the ISP consists of different levels, then each level must be defined to have the same common ground for discussions. We have defined the management level as suggested by Von Solms & Von Solms (2006) with three sub-level: Strategic, tactical and operational.

The strategic level represents the overall ISP. It sets the basis for directing all management levels while receiving compiled reports from the tactical level. The accumulation of reports gives the executive management oversight over to which extent the organization is aligned with business objectives, which is used to improve decision-making.

The tactical level consists of two key components: the potential future state by risk management and the current state of security controls. The tactical level receives direction from the strategic level and directs the operational level by enforcing policies and receiving measurement data about conformance. The component “current state of security controls” is determined by collecting data from different sources based on all types of security controls, which can be organizational, technological and physical. The component “potential future state by risk management” is determined by assessing potential risk based on data from the “current state” and the predicted future threat landscape. It is important to address all elements of risk like adversarial threats, natural occurrences, human-related incidents and opportunities (Posthumus & Von Solms, 2004). Then, the tactical level compiles all measurement data from the two key components into a report which is submitted to the strategic level.

The operational level consists of the individual security controls grouped by organizational, technological and physical types. The operational level receives direction from the tactical level, executes according to policy and produces measurement data indicating the conformance level. The most important aspect is that every security control must address people, process, technology (Posthumus & Von Solms, 2004; Veiga & Eloff, 2007) and suppliers (Slayton, 2021; Culot *et al.*, 2021), which gives a holistic understanding of the ISP. Every organization is different, and not everyone who works with access control is organized in the same department, and hence may have different managers; this is what Palmberg (2009) refers to as the functional groups. To address this issue, it is necessary to remove barriers between functional groups by organizing cross-functional team members, which Palmberg (2009) defines as process management. By organizing processes, it is necessary to define roles, and most importantly to avoid that process owners have conflicting authority with functional group leaders. Process owners are accountable for their respective processes and must ensure alignment with defined policies. This means that the process owner must oversee performance measurement, ensuring continuous improvement and the desired posture level by leading members in the process team (Palmberg, 2009).

4.3 RQ3 - How should the information security posture be communicated to executive management, and used for better decision-making?

We have discussed how to organize a reporting structure, but even so there is no widely accepted method on how to report. Below, we propose some reporting concepts and define criteria for different ISP levels corresponding to categories. An example is provided in table 3:

| Colour code | Posture category | Criteria |
|-------------|-------------------|----------------------|
| White | Excellent posture | 80%-100% conformance |
| Green | Good posture | 60%-79% conformance |
| Yellow | Moderate posture | 40%-59% conformance |
| Orange | Poor posture | 20%-39% conformance |
| Red | Critical posture | 0%-19% conformance |

Table 3. Posture levels and criteria

By using posture criteria, a process manager can assign a posture level to the ISP they are accountable for. The conformance is determined by an average score from the metrics collected from different postures according to a pre-set baseline. This sets the basis for decision-making since it can be used to discuss which posture should be prioritized to reach a higher conformance level, or it can be used for identifying risk. Since each posture consists of data about conformance levels and is organized in a manner that can aggregate to different management levels, it is possible to discuss it on any level. This model can be integrated into a dashboard, which automatically monitors and collects measurements. By implementing a dashboard, the executive management has oversight and can oversee the ISG program.

As already discussed it is important to address uncertainty, where an example is provided in table 4. The uncertainty assessment should be used in conjunction with posture-level criteria:

| Uncertainty level | Confidence level |
|-------------------|------------------|
| High | 0%-24% |
| Medium | 25%-59% |
| Low | 60%-79% |
| Minimal | 80%-100% |

Table 4. Correspondence between uncertainty and confidence levels

The purpose of considering the uncertainty levels is to communicate how confident you are in the data from the ISG program. For instance, if you report a moderate ISP, then you must also state how confident you are in that assessment. Things that can affect the confidence level e.g., the amount and how you collect data, how you process data, method and the validity of the assessment. Understanding the uncertainty means that you acknowledge it and can manage uncertainty to an acceptable level of confidence, which could lead to better decision-making. The principle is that it is unsafe to make important decisions based on highly uncertain ISP assessments.

5. Limitation

While this research contributes by defining, adding more meaning and conceptualizing ISP, it is important to discuss the limitations of this research.

First, regarding the method for collecting data, there is the possibility that the search strings and engines have not been optimal. However, we argue that the quality of data collection was fairly good, because from the reference list the term ISP was mentioned directly and indirectly in 8 research papers, while 2 of the research papers had defined the term, as well as 1 non-research web article. From the initial search, even more research papers mentioned the term ISP, but these articles were irrelevant for this research. There is a possibility that ISP has been discussed and defined by other researchers and it is possible that we could have found more research papers by performing more iterations of data collection. With a data collection period from 17.01.2022 until 24.02.2022, we judged that we had reached what Crang & Cook (2007) defines as the “theoretical saturation”. This means that it might be possible to find research papers with similar findings possibly explained in different ways. However, this would probably not result in a significant additional contribution to our research. Another strategy could be to define a new terminology instead of using ISP, to get a new perspective. However, since the term has not been elaborated on and is a widely used term, we found it beneficial to add more meaning and context to the existing term than to define a new term.

Another reason is that very few research papers have discussed how to implement an ISG program so that the executive management can have oversight over all information security activities. From the data collection, we found only theoretical frameworks, and papers discussing proposed frameworks/standards are generic and do not provide any methodical validation. It is possible that the chosen search strings or searching techniques were suboptimal, meaning that there is still a possibility that there are some research papers on this matter that have not been covered.

Finally, the proposed framework for ISP is a theoretical contribution and has not been validated or tested for practicality. Even so, our research expands and elaborates on how to organize an ISG program, supports other researchers’ contributions, and it addresses the need for a framework that describes “how” to organize and communicate an ISG program.

6. Conclusion

This research argues that potential future state and uncertainty are also key components for understanding ISP besides status, and discusses how these components can be related and organized. We argue that ISP can be separated into different levels like a reporting structure, which in turn determines the overall ISP. Then, we suggested how to report ISP levels and communicate uncertainty levels. There might still be some limitations in our research, in which case our contribution can form the basis for further research. Potential future research could be to implement this framework by using action research which could be used to learn and improve the framework and elaborate on “how” to organize an ISG program, hence this research is the first step in this journey.

7. References

- AlGhamdi, S., Win, K., & Vlahu-Gjorgievska, E. (2020) "Information security governance challenges and critical success factors: Systematic review", *Computers & security*, 2020-12, Vol.99, 102030, doi:10.1016/j.cose.2020.102030.
- Anu, V. (2021) "Information security governance metrics: a survey and taxonomy", *Information Security Journal: A Global Perspective*, 2021-05-16, pp 1-13, doi:10.1080/19393555.2021.1922786.
- Crang, M., & Cook, I. (2007) *Doing Ethnographies*, SAGE Publications Ltd, London.
- Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021) "The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda", *The TQM Journal*, Vol. 33, No. 7, 2021, pp 76-105, doi:10.1108/TQM-09-2020-0202.
- Johnston, A., & Hale, R. (2009) "Improved security through information security governance", *Communications of the ACM*, 2009-01-01, Vol.52 (1), pp 126-129, doi:10.1145/1435417.1435446.
- Kitchenham, B. (2004) "Procedures for Performing Systematic Reviews", *Keele University Technical Report TR/SE-0401*.
- Mills, J., Bonner, A., & Francis, K. (2006) "The Development of Constructivist Grounded Theory", *International Journal of Qualitative Methods*, 2006, 5(1), pp 25-35, doi:10.1177/160940690600500103.
- NIST. (2022) "NIST Information Technology Laboratory", [online], Computer Security Resource Center - Glossary: https://csrc.nist.gov/glossary/term/security_posture.
- Palmberg, K. (2009) "Exploring process management: are there any widespread models and definitions?", *TQM journal*, 2009-02-27, Vol.21 (2), pp 203-215, doi:10.1108/17542730910938182.
- Pérez-González, D., Preciado, S., & Solana-Gonzalez, P. (2019) "Organizational practices as antecedents of the information security management performance: An empirical investigation", *Information Technology & People*, West Linn, Vol. 32, Iss. 5, (2019), pp 1262-1275, doi:10.1108/ITP-06-2018-0261.
- Posthumus, S., & Solms, R. (2004) "A framework for the governance of information security", *Computers & Security* (2004) 23, pp 638-646, doi:10.1016/j.cose.2004.10.006.
- Siponen, M., & Willison, R. (2009) "Information security management standards: Problems and solutions", *Information & Management* 46 (2009), pp 267–270, doi:10.1016/j.im.2008.12.007.
- Slayton, R. (2021) "Governing uncertainty or uncertain Governance? Information Security and the challenge of cutting ties", *Science, Technology & Human Values* 2021, Vol. 46(1), pp 81-111, doi:10.1177/0162243919901159.
- Von Solms, B., & Von Solms, R. (2004) "The 10 deadly sins of information security management", *Computers & security*, 2004, Vol.23 (5), pp 371-376, doi:10.1016/j.cose.2004.05.002.
- Von Solms, B., & Von Solms, R. (2005) "From information security to...business security?", *Computers & security*, 2005, Vol.24 (4), pp 271-273, doi:10.1016/j.cose.2005.04.004.
- Von Solms, R., & Von Solms, S. (2006) "Information Security Governance: A model based on the Direct–Control Cycle", *Computers & security* 25 (2006), pp 408–412, doi:10.1016/j.cose.2006.07.005.
- Soomro, Z., Shah, M., & Ahmed, J. (2016) "Information security management needs more holistic approach: A literature review", *International journal of information management*, 2016-04, Vol.36 (2), pp 215-225, doi:10.1016/j.ijinfomgt.2015.11.009.
- Tashi, I., & Ghernaoui-Helie, S. (2009) "A Security Management Assurance Model to Holistically Assess the Information Security Posture", *2009 International Conference on Availability, Reliability and Security*, 2009-03, pp 756-761, doi:10.1109/ARES.2009.28.
- Veiga, A., & Elof, J. (2007) "An Information Security Governance Framework", *Information Systems Management*, Fall 2007, 24, pp 361-372, doi:10.1080/10580530701586136.
- Whitman, M., & Mattord, H. (2014) "Information Security Governance for the Non-security Business Executive", *Journal of Executive Education*, 2014, 11(1), pp 97-111.
- Williams, G. (2012) "Cost effective assessment of the infrastructure security posture", *7th IET International Conference on System Safety, incorporating the Cyber Security Conference 2012*, 2012, p.1B4, doi:10.1049/cp.2012.1503.
- Young, R. (2008) "Defining the information security posture: an empirical examination of structure, integration and managerial effectiveness", *University of North Texas, Unpublished PhD Thesis*, [online], https://www.researchgate.net/publication/228413655_Defining_the_information_security_posture_an_empirical_examination_of_structure_integration_and_managerial_effectiveness.

Paper II

Informasjonssikkerhetsledelse - En holistisk tilnærming

Tran, Dinh Uy

Published by *Cappelen Damm Akademisk*, March 2023, ISBN/EAN:9788202754648.

Abstract

Norsk: Stadig hyppigere dataangrep mot organisasjoner og bedrifter har vist at manglende sikkerhetstiltak kan være svært kostbart og dessuten kan føre til omdømmetap for virksomhetene. Hittil har man gjerne sett på informasjonssikkerhet utelukkende som en del av IKT-faget, men nå ser vi en økende forståelse av at informasjonssikkerhet bør være en integrert del av virksomhetsstyringen. Fremtidens informasjonssikkerhetsspesialister bør altså ha god virksomhetsforståelse i informasjonssikkerhetsledelse. Med en holistisk tilnærming får leseren en bred og holistisk tilnærming til fagområdet informasjonssikkerhetsledelse. Den legger vekt på betydningen av både personlig utvikling, kunnskap innen ledelsesfag og god kommunikasjon. Bokens primære målgruppe er bachelor- og masterstudenter som studerer informasjonssikkerhet, men den kan også være aktuell for studenter innen informatikk, ledelse og HR, samt ansatte i næringslivet som ønsker å oppdatere sin kunnskap om informasjonssikkerhet eller som har ambisjoner om å jobbe med informasjonssikkerhetsledelse.

Informasjon om boken finner du her: [Cappelen Damm](#)

Link til e-bok finner du her: [E-bok versjon](#)

De første 20 sidene av boken finner du her: [Bla i boken](#)

English: The growing trend of cyber-attacks against organisations and businesses has shown that inadequate security measures can be costly and lead to a loss of reputation for organisations. Until now, information security has predominantly been seen as part of ICT, but now we see a growing understanding that information security should be an integral aspect of business activities. The information security specialists of the future should therefore have a good understanding of business. Information Security Management - A Holistic Approach gives the reader a broad and holistic approach to the field of information security management.

II. Informasjonssikkerhetsledelse - En holistisk tilnærming

It emphasises the importance of personal development, knowledge of management subjects and good communication. The book's primary target audience is bachelor and master's students studying information security, but it can also be relevant for students in the fields of informatics, management and HR, as well as business professionals who want to update their knowledge of information security or who have ambitions to work with information security management.

Information about the book can be found here: [Cappelen Damm](#)

Link to the e-book can be found here: [E-book version](#)

The first 20 pages of the book can be found here: [Flip through the book](#)

Paper III

Business Language for Information Security

Tran, Dinh Uy, Jøsang, Audun

Furnell, S., Clarke, N. (eds) Human Aspects of Information Security and Assurance. HAISA 2023. IFIP Advances in Information and Communication Technology, vol 674. Springer, Cham.



Business Language for Information Security^{*}

Dinh Uy Tran^{**1[0000-0001-5691-7641]} and Audun Jøsang^{1[0000-0001-6337-2264]}

University of Oslo, 0373 Oslo, Norway

Abstract. Prominent standards and frameworks for information security clearly state that business aspects on the one side, and technical aspects on the other, are equally important for the management of cyber security. Organisations with a relatively low maturity level in security management typically consider information security primarily as a technological issue. For those organisations, information security might not get the necessary support from top-level management because they are predominantly focused on business aspects, and are blind to the role information security plays for business. To obtain support from top-level management the information security practitioners need the skills to influence and help relevant stakeholders to understand how information security can support business objectives. In this debate, it is often argued that it is important to speak the language of management. This means that information security practitioners should learn how to translate technical terms to a business context, so top-level management can understand what it means for them. However, this debate has mostly focused on the importance of speaking the “Business Language for Information Security (BLIS)” but has not elaborated on what this language consists of and how to learn it. This paper proposes BLIS and a framework for how to learn it. By mastering BLIS, security professionals can articulate arguments that top-executive management can easily understand and act on. Therefore, we argue that taking a learning module on BLIS will be valuable and useful for the next generation of students in information security. Said briefly, learning BLIS will help students understand how information security can support business, and also how this can be explained to others.

Keywords: Business Language for Information Security · Information Security Governance · Information Security Management · Information Security Reporting.

1 Introduction

Information security is receiving increased attention through wide media coverage of hacking and cyber attacks. From these incidents, we learn that “hacking”

^{*} Published at the Human Aspects of Information Security and Assurance. HAISA 2023. IFIP Advances in Information and Communication Technology, vol 674. Springer, Cham., pp. 57–68.

^{**} Supported by Sykehuspartner Trust.

can have dire consequences for businesses, and hence is not only a technical issue. Information security needs to be seen both as a business issue as well as a technical one. Top-level management therefore needs an understanding of how information security actually supports business objectives.

The meta-study by AlGhamdi *et al.* [18] suggests that effective management and governance of information security require top-level management support and commitment. Their study is based on a survey of 60 papers where top management support is listed as 1 of 34 critical success factors. This is supported by Soomro *et al.* [16], who based on their meta-study stated that a lack of top-level management support reduces the effectiveness of information security efforts in an organisation. The authors argue that information security managers should involve top-level management while adopting a holistic approach to information security. This is precisely one of the requirements expressed by ISO/IEC 27001:2022 [35], which is a well-recognized standard for establishing an Information Security Management System (ISMS). Requirement 5.1 from ISO/IEC 27001:2022 [35] specifies that top management shall demonstrate leadership and commitment to the ISMS. A risk report from the The Directorate of e-health [36] under the Norwegian Ministry of Health and Care, stated that 88% of public healthcare institution have established an ISMS. The report also states that 22% of security incidents occur because of the lack of prioritisation of information security work, 33% of incidents occurred due to the lack of security processes, and one third of all public institutions detects security incidents by accident. Basically, these 88% of the health care institutions having implemented an ISMS should have top management support, but security incidents still occur because of the lack of prioritisation. This could indicate that the top management does not understand how information security can support the business, which is quite alarming when the national strategy for digital security in Norway [37] requires that organisations adopt well-known standard in ISMS such as ISO/IEC 27001:2022 [35].

The main motivation for this research is to overcome the difficulty that security specialists have in communicating how information security supports business objectives. The goal of understanding and explaining how information security supports business is to ensure that information security gets adequate prioritisation, and that management commitment is not simply signing off the ISMS documents without any real commitment. Researchers such as Karanja [13], Jirasek [14], and Johnston *et al.* [17] argue that information security management practitioners should talk the same “language” as that of top-level management and communicate in a clear and simple way how information security is aligned with business objectives. However, these researchers do not discuss how this “security business language” can be learned and used to influence top-level management to obtain support and commitment.

This research proposes a method for communicating information security in way the top management understands and hence results in management commitment. Our observation is that many researchers discuss this topic either directly or indirectly, and that the term “Business Language” is commonly used by both

researchers and practitioners. For the present paper, we will use the term “Business Language for Information Security”, for which we also provide a definition. Then, we will discuss what BLIS should consist of, which represents the theoretical framework for learning BLIS. This paper starts with a brief review of related research on this topic. Next, we describe the research method and how collected papers were analyzed and compared. Then, the results and discussion of the findings are presented. Finally, the paper provides some concluding remarks and proposes ideas for future research.

2 Background and related research

Information security researchers and practitioners have acknowledged the importance of communication skills to make information security understandable for top-level management. Whitman & Mattord [12], Jirasek [14], Fitzgerald [20], Harkins [22], and Johnston *et al.* [17] argue that information security practitioners should speak the language of business in a way that top-level management can easily understand. Schinagl & Paans [7] argue that experts tend to articulate their technical knowledge in a way that non-experts find difficult to grasp, while for peer experts, the same way of articulating technical issues is self-evident. Such cases of “system language” are typically used and understood within a group of experts, but represent a barrier to understanding for outsiders. Translating the system language of information security into business language will help non-experts understand how information security affects business. Karanja [13] also uses the term “business language” to describe the same matter. Researchers such as Ashenden & Sasse [15, 1], Soomro *et al.* [16], AlGhamdi *et al.* [18], and Rainer *et al.* [11] argue that effective communication is needed to ensure a common understanding between Information Security managers and top-level management.

There is a general consensus between researchers discussing communication, the language of business, and business language. However, it is often the case that researchers use different terms to discuss the same topic, which can lead to confusion. The lack of a standardised definitions is typically the root of the problem, which makes it necessary for practitioners to learn that different terms often mean the same thing. In this paper, we use the term “Business Language for Information Security”. As mentioned, the concepts that BLIS covers have been mentioned by different researchers, but we have not found any publication elaborating specifically on the interpretation of BLIS and how it can be applied. For instance, what is the business aspect of BLIS? What communication skills should be a part of BLIS in a way that is useful for communicating with top-level management? Our observation is that publications indirectly mentioning BLIS are related to Information Security Governance (ISG), Information Security Management (ISM), and the role of the Chief Information Security Officer (CISO). Unsurprisingly, these topics are related to business, and the CISO is usually a part of top-level management, or acts as an advisor related to information security. Understanding ISG, ISM, and the role of CISO provides the

basis for defining what BLIS should consist of. A clear definition of BLIS and a method to learn it will prepare the next generation of students for working on information security in business settings.

The purpose of ISG is to establish a governance structure for top-level management to direct and control information security activities to support business objectives (Posthumus & Solms, [25]). This means that ISG is a tool for CISO to get oversight over the information security activities and how they perform according to business objectives, also known as information security posture (ISP). By monitoring the ISP, the CISO has oversight over risks, uncertainties, and the status of the ISG program and can use this insight to ensure that top-level management takes well-informed decisions (Tran & Jøsang, [31]). To ensure that ISG is aligned with business objectives, the CISO needs to manage personnel, processes, and technology related to Information Security by overseeing and managing daily security activities, which is known as ISM, and is an integral component of ISG (Solms & Solms, [26]).

Ashenden [15] argues that ISM is about managing people, since people are the ones who use processes and technologies to achieve business objectives. When dealing with the human aspects of management, it is beneficial to have an understanding of different fields of management, organisational behaviour, and culture. Soomro *et al.* [16] suggest that ISM requires a good understanding of organisational structure to facilitate reporting structure, clear authority, and efficient communication and processes. To manage people, it is beneficial to develop leadership and interpersonal skills for motivating and influencing people, but also for effectively communicating with top-level management (Whitten, [21]). Relevant research indicates that for BLIS to be effective, it should include elements from business, leadership, soft skills, communication, ISG, and ISM.

3 Research method

A systematic literature review based on a procedure developed by Kitchenham [30] was conducted and split into two phases. The first phase was to collect papers related to BLIS from three digital libraries, while the second phase consisted of identifying additional papers based on analysing selected papers from the first phase. The chosen digital libraries were Scopus, Web of Science, and Google Scholar, which include a vast amount of papers on different areas of Information Security. The search keywords used are: “Business Language for Information Security”, “Business Security Language” and “Business Language for Cyber Security”. The search was conducted in September 2022, and the results were sorted based on relevancy. To the best of our abilities, there is no prior research specifically on what we call Business Language for Information Security. The search returned from the first phase is provided in table 1:

We then screened the title and abstract accordingly to identify papers that could discuss the topic, which identified 32 papers for which we conducted a full-text assessment. During the full-text assessments, we applied principles from Grounded Theory (Mills *et al.*, [29]) because there is no prior research on BLIS.

Table 1. Data collection - BLIS.

| Search keywords | Web of Science | Scopus | Google Scholar |
|--|----------------|--------|----------------|
| “Business Language for Information Security” | 542 | 855 | 3520000 |
| ‘Business Security Language’ | 1173 | 1708 | 3550000 |
| “Business Language for Cyber Security” | 66 | 91 | 274000 |

In the Grounded Theory, a researcher seeks to construct a theory from examining data, while the researcher has limited knowledge or only few predetermined ideas. Because of the limited literature on BLIS, Grounded Theory was suitable for this research as a method to generate new ideas and gain better understanding of this topic.

During the full-text assessments, comparing similarities from different contributions by different researchers we could identify common characteristics, and started to translate these findings into codes and categorizations. This in turn helped us generate and refine our research questions, and we developed inclusion and exclusion criteria to help us identify relevant research papers. The inclusion and exclusion criteria were constantly evolving until we reach the point of theoretical saturation (Crang & Crook, [32]). Saturation means that we had reached a point where we could possibly collect additional similar findings, but that simply explain the same concepts and ideas in different ways, which would not likely contribute more to our research.

The initial step when conducting a full-text assessment with principles from Grounded Theory was to generate open coding (Glaser, [33]), which is a theoretical analysis from the research data and why these are relevant to this research. Which in turn resulted in 47 open codes, this forms the basis to identify core categories. These five core categories are Business, Communication, Information Security, Soft Skills, and Pedagogy. Then, we transferred the open codes to their respective categories.

Both the core categories and open codes functions as our inclusion and exclusion criteria’s, for identifying relevant papers. Afterwards, we used another form of coding called axial coding (Strauss & Corbin, [34]) to make links between the open codes and core categories. These links are used to identify interconnections and if these topics are discussed directly or indirectly by other researchers. To link these codes together, we used a diagramming tool, Obsidian to give us an oversight over the complex interplay from the different researchers, which could aid us in our research.

A result of the full-text assessment from the 32 papers, only 24 of these papers were relevant. However, based on the first iteration, we identified 12 additional papers from our initial full-text assessment and then performed the same research procedures on these papers. We decided that it was only needed to perform the research procedure twice, since our observation is that we found the same results but explained differently, hence theoretical saturation as discussed earlier.

This resulted that 36 papers and 47 codes were deemed relevant for BLIS. The core categories are Business (13 codes), Communication (13 codes), Information Security (8 codes), Soft Skills (8 codes), and Pedagogy (5 codes). After two iterations of this research method we could find the gap of existing research on BLIS. Based on these limitations this papers will discuss two research questions:

1. What should the definition of Business Language for Information Security be?
2. What should the theoretical framework for learning the Business Language for Information Security consist of?

3.1 Potential weaknesses of study

Potential weaknesses of this study are related to data collection and developing codes, because only one of the authors was involved in this process. This means that we could have missed relevant research papers that potentially are related to BLIS. However, to address this weakness, we paid attention to the use of databases with most relevant papers and perform the same keyword searches on all databases. Then, we developed codes with corresponding categories to establish an include and exclusion criteria to provide a consistent method of data collection. We argue that the quality of data collection was fairly good, and that the identified 36 papers discuss elements directly or indirectly related to BLIS, and we reached the point of theoretical saturation, as mentioned earlier.

Another potential weakness could be related to defining the different core categories, which later becomes the main components of the theoretical framework for BLIS. Another researcher who performs the same research method would most likely develop different core categories. Which is natural since every researcher has different backgrounds and experiences, which could lead to different views and interpretations. This paper is to the best of our knowledge the first to argue the need for BLIS and present a theoretical framework to learn, and every innovation needs a start and then refined over time. However, to address this weakness, we have to the best of our abilities tried having limited predetermined ideas as possible before the research and let the research data generate a new theory, which is why we used the grounded theory.

A potential minor weakness of this study is our assumption about management commitment from the healthcare sector in Norway, which based on the report [36] was assessed to not give priority to security. Our study indicates that the top management have a relatively limited understanding of how information security supports business objectives. We acknowledge that there could be other reasons for that, like e.g., the health institution has done risk assessments with the conclusion that security should not be prioritised. However, these aspects are not discussed in this study, and there could also be differences in other sectors and countries. Based on our research, we argue that there is a need for helping top management in organisations to understand how security supports the business, which could lead to improved management commitment. Most literature and standards discuss the importance of management commitment, but not

how to gain that commitment, which is precisely the focus of the present study. Either way, if our assumptions about the report is correct or not, this research can give professionals better awareness about the business side and increase the likelihood of gaining top management commitment.

4 Results

This section describes our critical analysis of collected papers and presents our results.

4.1 Definition

From the relevant papers, we observe that the common element of BLIS is that information security practitioners should speak the same language as business practitioners. We agree that one of the outcomes of BLIS is related to “speaking the same language as business people” or “translating technical language to business language”, but we argue that it is not only for communications. We find translating “technical language to business language” more precise than “speaking the business language”.

We argue that the aim of BLIS is not just to speak the business language, but to make others understand the importance of information security for business. Primarily, it is absolutely necessary to understand relevant business fields. Secondly, information security practitioners should have solid competence in relevant information security fields. Having solid competences should help practitioners have a better foundation to translate the information security language into business language in a way that is simple to understand. Thirdly, it is important to have learned the basic elements of communication science, which includes soft or interpersonal skills, but we added soft skills as a fourth aspect to emphasise its importance. Finally, it is also about learning pedagogy to teach and merge these components practically and efficiently.

These 5 components of BLIS are what we discovered by conducting full-text assessments, and we argue that it is necessary to learn all these components to master BLIS. We argue that learning BLIS can help the next generation of practitioners get a better understanding of skills needed to improve and understand how information security supports business, and develop communication strategies with the help of soft skills for different target users and not limited to top-level management. Pedagogy is to learn how to teach different aspects of BLIS and is not limited to speaking the business language.

We therefore, argue that BLIS is a distinct field within information security that is essential for effectively managing information security in a professional business setting. Based on the discussion above, we define BLIS as follows:

“Business Language for Information Security is a field that merges relevant fields from Business, Communication, Information Security, Soft Skills and Pedagogy for practical use of Information Security in a professional business setting”

We argue that this definition captures all the relevant aspects of BLIS, and is not limited to communicating with top-level management. We argued that BLIS is a distinct field within information security, and is applicable for many use cases. To effectively practice BLIS, a structured approach to learning is needed for merging the 5 elements it contains. It needs dedication to learn BLIS, which cannot be compared to simply “speaking” the business language. Also, we could have given a new definition instead of using BLIS, but we found it more beneficial to add more meaning and make the existing term more useful. Next, we will discuss the content in the 5 key components of BLIS.

4.2 Business and Information Security

To identify relevant business fields, we must analyse fields in information security that have an intersection with and identify different use cases in which an information security manager can be involved with top-level management. Fields like ISG and ISM are well established through numerous standards, and a consensus among researchers is that ISG is a subset of Corporate Governance (Posthumus & Solms, [25]; Soomro *et al.*, [16]). This indicates that it is beneficial for Information Security practitioners to learn about Corporate Governance, which also includes Corporate Risk Management. The same can be said about ISM, which is a subset of ISG and Corporate Governance that it can be beneficial to learn management fields since we are dealing with managing people from different parts and fields in an organisation, not limited to Information Security practitioners. Whitten [21] suggested researching the connections between Mintzberg’s [27] managerial work roles with the CISO role and our observation is that it is relational. Mintzberg’s [27] defined three manager roles; Interpersonal, Informational, and Decisional, and each role has separate sets of managerial activities. CISO should learn to motivate, develop relationships with other co-workers and build working relationships with other managers through interpersonal contact to ensure effective ISM and organisational culture, which is aligned with Mintzberg’s [27] description of “Interpersonal role”.

Soomro *et al.* [16] and Ashenden & Sasse [1] argue that competence in organisational structure is important to facilitate efficient workflow and a reporting structure. AIGhamdi *et al.* [18] argue that information security requires establishing cross-organisational collaboration and can be interpreted as there is a need for competence in process development, which is a view supported by Whitman & Mattord [12], Karanja [13] and Jirasek [14]. Having competence in organisational structure and process development can help CISOs develop effective security metrics, which Anu [19] argues could enable monitoring the overall success of the ISG program. Monitoring and having oversight over information security activities from the ISG program is similar to Mintzberg’s [27] description of the “Informational role”.

Finally, a CISO supports top-level management in decision making and devises strategies to achieve business objectives and can act as a negotiator by developing business cases (Rainer *et al.* [11]) to gain needed resources, which is similar to Mintzberg’s [27] description of “decisional role”. Johnston *et al.* [17]

argue that it is important to develop interpersonal skills to understand different personality characteristics, and in a management context, we know that every person is different and managers should learn to use different management roles depending on the situation. Hersey *et al.* [28] have developed a framework called “Situational Leadership” to manage different types of persons or stakeholders, which can be useful to handle interpersonal contact.

4.3 Communication and Soft Skills

The field of communication, which includes soft skills or interpersonal skills is related to practicing management as we discussed, but not limited to management, as it applies to other types of people as well. As discussed earlier, the purpose of communication skills is to create a common understanding (Whitman & Matford, [12]; Ashenden & Sasse, [1]; Harkins, [22]; Hooper & McKissack, [23]). Common understanding can be obtained from “speaking the same language as recipients” (Johnston *et al.* [17]), but also includes other methods like process modelling and rhetoric.

According to Moyón *et al.* [10], process modelling is a visual description to make information security easier to understand for non-security practitioners. For instance, Moyón *et al.* [10] translated a complex security requirement from IEC 62443-4-1 standard into Business Process Modelling Notation (BPMN), which is a type of process model. Then, they interviewed 16 industry experts, of which 14 claimed that the BPMN was easier to understand. This indicates that process modelling can be useful for communicating and unsurprisingly, there are different models for different purposes like the following: Unified Model Language (Sechi *et al.*, [9]), SecureBPMN (Brucker, [5]; Alotaibi, [4]; Altuhhova *et al.* [6]) and Enterprise Architecture Management (Abbass *et al.*, [8]).

Johnston *et al.* [17] argue that learning the field of Rhetoric can be useful to improve the understanding of information security to non-experts. Rhetoric is the practice of communicating a tailor-made message to the recipient, to persuade them to perform a specific set of behaviours or activities. Design tailor-made messages require an understanding of personality characteristics, behaviour, and social skills to interact with different people (Kayworth & Whitten, [24]).

There are different rhetorical techniques, where e.g. the security industry tends to use “fear” to sell information security according to Harkins [22]. The same matter is discussed by Johnston *et al.* [17] under the term “fear appeal theory”, which is a way of “scaring” others to behave in a specific way. Harkins [22] argues that relying on “fear” can have the opposite effect because people do not want to listen to negativity, with the effect that over time information security will lose credibility. Harkins [22] argues that we instead should focus on “solutions”. From our understanding, focusing on solutions is the opposite of “fear appeal theory” and we define it as an “opportunistic approach” which is a way of proposing solutions to emphasise that information security is a business enabler.

We agree with Harkins [22] arguments that in general it is preferable to use the “opportunistic approach” as opposed to what Johnston *et al.* [17] calls “fear

appeal theory”. However, we still think that both of these methods can be useful, depending on the situation, and a combination can help to illustrate both sides of the challenge with information security. Since people are different, the best method to use typically depends on the individual personal characteristics, which means that some prefer and understand rhetoric based on the “opportunistic approach” while other prefer the approach of the “fear appeal theory”. The time frame can be a factor for deciding which approach to use. As an example, in situations of handling security incidents where decision-making must happen swiftly and where the focus is short term, it might be better to use “fear appeal theory”. The “opportunistic approach” is probably better suited for negotiating business or strategic plans and long-term planning since it sets an optimistic tone while negotiating.

4.4 Pedagogy

Pedagogy is about how to structure BLIS in a manner that makes it easier to learn and teach efficiently. We argue that utilising BLIS needs dedication and combining many different fields, and is not as simple as speaking business language by using some business terms. A natural requirement for using business terms in communication with management is that the practitioner should have the foundational understanding of business concepts to discuss it critically. Simply focusing on learning terms but not having understanding could at worst result in a loss of credibility.

To develop BLIS and build a curriculum, it is important to have understanding of pedagogy, since it provides a basis for identifying appropriate teaching methods, and for constantly improving the program. Understanding pedagogy can also help the practitioners have a broader view and methods to teach others information security skills or build better culture.

Kolomiets & Konoplenko [2] suggest to use a “Business Game” which is a model based on “task-based learning”. This was taught by simulating different situations that could occur in student’s later professional life to build their experience before graduating. This can also be beneficial for learning BLIS.

Drevin *et al.* [3] also suggest a linguistic approach to learning information security. This approach consists of developing a language around a topic, and measuring understanding with a vocabulary-measuring instrument in a group to test their knowledge and understanding of the language. This method is also applicable for learning BLIS since it consists of many different fields and is an excellent way to test the students and their understanding.

Based on the above discussion we see that BLIS is far too complex to be viewed just as “speaking” the business language, Hence, BLIS should be seen as a distinct field within information security, which should become a part of the “common body of knowledge” for information security practitioners and the next generations of students.

5 Future work

This paper proposes a theoretical framework for learning BLIS. The framework still needs to be validated for practicality, with its different components. The only way to understand another language is to learn it, and hence the next step should consist of letting a group of security professionals try it out in their working environment. The present study has focused on describing BLIS and benefits of learning it. We argue that students of information security need to learn how to communicate the importance that information security has for business, with the aim of obtaining management support and commitment. This paper describes a basis for developing a curriculum based on our proposed theoretical framework.

Our ongoing work will be to validate BLIS and improve the theoretical framework. We will interview CISOs to collect real business scenarios which will become learning material for the students, called "Security Business Games". Another activity will involve students who are attending continuing education and professional development by first presenting a business game without teaching BLIS, then to teach them BLIS followed by a similar, but different, business game. The aim will be to compare the data and conduct interviews on their experiences with BLIS. This represents a method to empirically validate BLIS and improve the BLIS curriculum.

Additionally, we will interview CISOs to gain more insight on what should be the core components and sub-components of BLIS, based on their experience from real business settings. This will allow us to compare data from interviews with the experience from applying BLIS in different business games, which provides empirical evidence to improve and validate the different components of BLIS. Each component and sub-component represents its own complex field that needs investigation to ensure that BLIS becomes practical and useful for information security professionals.

6 Conclusion

In this study, we have defined the BLIS and proposed a theoretical framework for learning it. We argue that BLIS is not for only communicating with management, but also a distinct field within information security. We argue that learning BLIS will help professionals and students with the practical use of information security in a business setting. The key components of BLIS are Business, Information Security, Communication, Soft Skills, and Pedagogy. These components are essential to learning and using BLIS in a business setting. We have elaborated to some extent on what these components consist of, which can be used to develop a curriculum to teach future students.

This research aims to gain better understanding and improve the business aspects of information security. The fundamental assumption is that information security is an essential business issue, and not just a technical issue. It is crucial to educate business leaders to understand this, and the purpose of BLIS is precisely to help security professionals in this endeavor. Generally, we believe that

BLIS is not just for communicating with management but is a way of integrating information security in business settings, and a way of defining information security as a core element of business management.

References

1. Ashenden, D., Sasse, A. CISOs and organisational culture: their own worst enemy?. *Computers & Security*, **39**, 396–405 (2013)
2. Kolomiets, S., Konoplenko, L. A model for teaching speaking English for Specific Purposes (information security) using business game. *Advanced Education*, **3**, 58–63 (2015)
3. Drevin, L., Kruger, H., Bell, A. & Steyn, T. A linguistic approach to information security awareness education in a healthcare environment. *IFIP World Conference On Information Security Education*, 87–97 (2017)
4. Alotaibi, Y. A Secure Business Process Modelling For Better Alignment between Business and IT. *2016 49th Hawaii International Conference On System Sciences (HICSS)*, 4793–4802 (2016)
5. Brucker, A. Integrating security aspects into business process models. *It-Information Technology*, **55**, 239–246 (2013)
6. Altuhhova, O., Matulevičius, R. & Ahmed, N. Towards definition of secure business processes. *International Conference On Advanced Information Systems Engineering*, 1–15 (2012)
7. Schinagl, S. & Paans, R. Communication barriers in the decision-making process: System Language and System Thinking. *Proceedings Of The 50th Hawaii International Conference On System Sciences*. (2017)
8. Abbass, W., Baina, A. & Bellafkih, M. Improvement of information system security risk management. *2016 4th IEEE International Colloquium On Information Science And Technology (CiSt)*, 182–187 (2016)
9. Sechi, F., Gran, B., Jørgensen, P., Kilyukh, O. Better Security Assessment Communication: Combining ISO 27002 Controls with UML Sequence Diagrams. *2022 IEEE/ACM 3rd International Workshop On Engineering And Cybersecurity Of Critical Systems (EnCyCriS)*, 49–56 (2022)
10. Moyón, F., Méndez, D., Beckers, K. & Klepper, S. Using Process Models to Understand Security Standards. *International Conference On Current Trends In Theory And Practice Of Informatics*, 458–471 (2021)
11. Rainer Jr, R., Marshall, T., Knapp, K. & Montgomery, G. Do information security professionals and business managers view information security issues differently?. *Information Systems Security*, **16**, 100–108 (2007)
12. Whitman, M. & Mattord, H. Information security governance for the non-security business executive. (2014)
13. Karanja, E. The role of the chief information security officer in the management of IT security. *Information & Computer Security*. (2017)
14. Jirasek, V. Practical application of information security models. *Information Security Technical Report*, **17**, 1–8 (2012)
15. Ashenden, D. Information Security management: A human challenge?. *Information Security Technical Report*, **13**, 195–201 (2008)
16. Soomro, Z., Shah, M. & Ahmed, J. Information security management needs more holistic approach: A literature review. *International Journal Of Information Management*, **36**, 215–225 (2016)

17. Johnston, A., Warkentin, M., Dennis, A. & Siponen, M. Speak their language: Designing effective messages to improve employees' information security decision making. *Decision Sciences*. **50**, 245–284 (2019)
18. AlGhamdi, S., Win, K., Vlahu-Gjorgievska, E. Information security governance challenges and critical success factors: Systematic review. *Computers & Security*. **99**, 102030 (2020)
19. Anu, V. Information security governance metrics: A survey and taxonomy. *Information Security Journal: A Global Perspective*. **31**, 466–478 (2022)
20. Fitzgerald, T. Clarifying the roles of information security: 13 questions the CEO, CIO, and CISO must ask each other. *Information Systems Security*. **16**, 257–263 (2007)
21. Whitten, D. The chief information security officer: An analysis of the skills required for success. *Journal Of Computer Information Systems*. **48**, 15–19 (2008)
22. Harkins, M. The 21st Century CISO. *Managing Risk And Information Security*, 139–153 (2016)
23. Hooper, V. & McKissack, J. The emerging role of the CISO. *Business Horizons*. **59**, 585–591 (2016)
24. Kayworth, T. & Whitten, D. Effective information security requires a balance of social and technology factors. *MIS Quarterly Executive*. **9**, 2012-52 (2010)
25. Posthumus, S. & Von Solms, R. A framework for the governance of information security. *Computers & Security*. **23**, 638–646 (2004)
26. Solms, S. & Solms, R. Information security governance. (Springer Science & Business Media,2008)
27. Mintzberg, H. Managerial work: Analysis from observation. *Management Science*. **18**, B97–B110 (1971)
28. Hersey, P., Blanchard, K. & Natemeyer, W. Situational leadership, perception, and the impact of power. *Group & Organization Studies*. **4**, 418–428 (1979)
29. Mills, J., Bonner, A. & Francis, K. The development of constructivist grounded theory. *International Journal Of Qualitative Methods*. **5**, 25–35 (2006)
30. Kitchenham, B. Procedures for performing systematic reviews. *Keele, UK, Keele University*. **33**, 1–26 (2004)
31. Tran, D. & Jøsang, A. Information Security Posture to Organize and Communicate the Information Security Governance Program. *Proceedings of the 18th European Conference On Management Leadership And Governance, ECMLG 2022*. **18**, 515–522 (2022)
32. Crang, M., Cook, I. & Others Doing ethnographies. (Sage,2007)
33. Glaser, B. Basics of grounded theory analysis: Emergence vs forcing. (Sociology press,1992)
34. Strauss, A. & Corbin, J. Basics of qualitative research techniques. (Citeseer,1998)
35. Standardization, I. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. (2022)
36. Helse, D. Overordnet risiko- og sårbarhetsvurdering for IKT i helse- og omsorgssektoren. (2019)
37. Regjeringen Nasjonal strategi for digital sikkerhet. (2019)

Paper IV

An Opportunity-Based Approach to Information Security Risk

Tran, Dinh Uy, Selnes, Sigrid Haug, Jøsang, Audun, Hagen, Janne

To appear in: The 4th International Workshop on Cyber-Physical Security for Critical Infrastructures Protection (CPS4CIP 2023).

An Opportunity-Based Approach to Information Security Risk *

Dinh Uy Tran^{**}[0000-0001-5691-7641], Sigrid Haug
Selnes^{***}[0009-0000-6051-794X], Audun Jøsang^[0000-0001-6337-2264], and Janne
Hagen^[0000-0001-5900-7061]

University of Oslo, Oslo 0373, Norway

Abstract. The traditional approach to Information Security Risk Management (ISRM) is to assume that risk can only affect businesses negatively. However, it is interesting to notice that the latest edition of the standard *ISO/IEC 27005:2022 Guidance on managing information security risks* provides a definition of risk that covers both positive and negative consequences. Hence, present and future business leaders can expect information security professionals in their organisations to report on positive aspects of information security risk in addition to negative risk, which is a rather new and radical idea. Since information security risk assessment has traditionally focused on threats, no guidelines currently exist for how to identify, describe or assess positive risk in the context of ISRM. The aim of this study is to describe an opportunity-based approach to information security risk. In addition, this paper discusses some limitations of how ISO/IEC 27005:2022 defines risk, and hence this paper also proposes a definition of positive risk in the context of ISRM. Finally, some strategies to describe and assess positive risk are described.

Keywords: Positive Risk · Opportunity · Information Security Risk Management · Information Security Governance · Cyber Security.

1 Introduction

Frameworks for Information Security Risk Management (ISRM) have traditionally focused on threats from a technological perspective. Standards, textbooks and industry certifications have mostly taken this perspective. In the last decade, however, information security has received increased attention from top-level management in organisations, due to the many distressing examples of cyber-attacks seriously affecting businesses. As a result, standards and frameworks have evolved to include controls and policies to help information security gain management support and align with business objectives, where the standard

* Published at the 4th International Workshop on Cyber-Physical Security for Critical Infrastructures Protection (CPS4CIP 2023).

** Supported by Sykehuspartner Trust.

*** Supported by the Raksha Project, funded by the Research Council of Norway.

ISO/IEC 27001:2022 Requirements for Information Security Management Systems is a prominent example ([4]). It is also noteworthy that the latest edition of the standard *ISO/IEC 27005:2022 Guidance on managing information security risks* ([7]) has expanded the definition of risk to include positive risk, which is a significant addition. This means that information security risk is not limited solely to negative risk, which is the traditional approach. There are three benefits of emphasising positive risk with regard to information security. The first benefit is that this could change the stereotypical assumption that information security practitioners tend to use fear to “sell” information security to managers, which is a negative way to communicate (Whitten, [3]). The second benefit is that this opens up new ways of communicate risk in the sense that it can be communicated both positively and negatively. The third benefit is that information security risk can be aligned with business risk, for which positive risk has been adopted since at least 2009, e.g. as described in *ISO 31000:2009 - Risk Management: Guideline*.

In a survey from ISO ([9]) the *ISO 9001 Quality Management* ([22]) management system standard was listed as the standard with the highest number of valid certifications, with 1,077,884 certified organisations worldwide, while *ISO 14001 Environmental management system* is the second most used, with 420,433 certified organisations. The standard *ISO/IEC 27001 Requirements for Information Security Management System* ([4]) is the fourth most used standard, with 58,686 certified organisations. These numbers do not include companies adopting these standards for their own benefit without seeking certification. This means that there is a high probability that a company will have designed its management system according to ISO 9001 ([8]), which also includes positive risk. Therefore, adopting a positive risk mindset for information security can help create a common understanding within the business, by using the same risk definition and principles. Even if these standards have added positive risk, a very limited body of literature discusses how to identify, describe or assess positive information security risk. Even the latest edition of *ISO/IEC 27005:2022* ([7]) still mainly focuses on negative risks and threats, even though the definition of risk has been updated to cover positive risks. The aim of the present study is to review existing research papers, standards and related literature to understand the current state of research in this field. We then describe our findings and use this knowledge to propose principles that can be applied to identify and assess positive risks in an information security context.

This paper is structured as follows. The next section gives a summary of the current state of research and functions as a theoretical foundation for our research. The third section describes our research method. The fourth section presents our findings and critical analysis, as well as an example of use of proposed methods. The last section provides a summary and concluding remarks.

2 Related research

This section gives a brief introduction to risk management and the current state of this field from a perspective that is relevant to our research and that discusses the research questions.

2.1 Risk management

Risk is defined as “*the effect of uncertainty on objectives*” in the standards ISO/IEC 27000:2018, [6]; ISO/IEC 27005:2022, [7]; ISO 31000:2018, [5]; ISO 9001:2015, [8], while NIST SP 800-37 ([11]) defines risk as “*A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence*”.

The definition of risk from NIST SP 800-37 ([11]) is similar to the previous version ISO/IEC 27005:2018 [15] which stated that “*risk is the potential that a given threat will exploit vulnerabilities of assets and thereby cause harm to the organization*”. Similar definitions of information security risk are expressed in mainstream textbooks for higher education and popular certifications such as CISM (Gregory, [14]) and CISSP (Harris & Maymi, [13]).

Risk management (RM) is a core component of information security governance. According to ISO 31000 [5], RM is defined as “*coordinated activities to direct and control an organization with regard to risk*”, while the RM process is defined as “*systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context and identifying, analysing, evaluating, treating, monitoring and reviewing risk*” (ISO/IEC 27000:2018, [6]). The importance of RM has led to the development of different standards and best practice approaches for implementing RM in an organisation, e.g., ISO/IEC 27005, ISO 31000, and NIST SP 800-37.

When surveying standards and guidelines for RM, researchers have identified a variety of limitations and challenges from both a theoretical perspective and for practical applications (Fenz et al. ([20]; Bergstrøm et al. [17]). For instance, frameworks are usually generic, with limited guidelines, and are not tailor-made for organisations (Mayer et al. [16]). ISRM frameworks tend to focus mostly on technological aspects, while the aspects of risk related to organisational aspects, human factors and processes are mentioned, but not elaborated on (Bergstrøm et al. [17]). This means that following the guidelines for ISRM might not cover risk at the organisational level, which could result in the organisation not having an oversight of the total risk and information security posture (Tran and Jøssang, [21]). This is a concern shared by Diefenbach et al. [18] and Abbass et al. [19].

By taking advantage of the relative flexibility of frameworks, as argued by Aleksandrov et al. ([22]), ISO/IEC standards can be integrated with other standards for management systems, which, when combined, provide a holistic approach to risk. This seems to be an approach adopted by many researchers,

and many papers exist that propose a more holistic approach to RM by integrating different frameworks. For instance, the lack of guidelines for aligning ISRM holistically and providing an oversight of business assets has contributed to researchers such as Mayer et al. ([16]), Diefenbach et al. ([18]) and Abbass et al. ([19]) proposing a model for integrating the Enterprise Architecture Model (EAM) with risk management frameworks such as ISO/IEC 27005 and ISO 31000.

Shamala et al. ([23]) express concerns about the risk assessment methodology due to the huge amount of information that it is typically necessary to process, for reliable conclusions to be drawn. This is why they propose integrating relevant information quality attributes derived from quality management in the process of gathering and assessing risk. This proposal could contribute to more reliable, verifiable and objective, and more accurate assessments of risk, to become a reliable factor in the decision-making process. Webb et al. ([24]) proposed a similar model based on adapting Endsley's situation awareness model into ISRM, with the goal of improving the process of gathering quality information to facilitate more accurate risk assessments. They called this an intelligence-driven approach to ISRM.

Riesco and Villagr a ([25]) argue that current RM frameworks are too static, and do not apply well to a landscape where information security risks and threats are constantly evolving and dynamic. From this perspective, they propose to integrate near real-time cyber-threat intelligence information (CTI) into ISRM frameworks. Integrating CTI into ISRM frameworks could provide better up-to-date risk-level calculations due to automation. They tested this framework on a national CSIRT (Computer Security Incident Response Team), and found that they were able to advance from the original (static) risk assessment approach used by the organisation, to a more dynamic approach. Other researchers, such as Putra and Mutijarsa ([26]) have implemented the ISMR process by integrating ISO/IEC 27005 for establishing the RM process, and then supplementing it with the NIST standard SP 800-30 Rev.1, used specifically for its method of conducting risk assessments. This design was implemented at the Indonesian national police command centre, which reported that it met their organisational needs for managing risk.

These are several interesting studies that adopt the integration of different frameworks to establish a more holistic approach to ISRM. However, our observation is that they all tend to focus on negative risk and not on positive risk. Examples are well-recognised industry standards and methodology such as ITIL 4 and FAIR (Factor Analysis of Information Risk). ITIL 4 ([36]) on the other hand, states that risk is something to avoid, but also emphasises that failure to use an opportunity can be a risk, which implicitly acknowledges positive risk. ITIL 4 references and supports the ISO 31000:2018 [5] definition, but still does not specify how to assess positive risk. The popularity of the FAIR methodology ([37]) is increasing rapidly and some enterprises such as Netflix, Hewlett-Packard Enterprise (HPE), National Aeronautics and Space Administration (NASA) and

many more, adopt this approach. However, FAIR has limited its methodology to negative risk, with its focus on threats, vulnerabilities and loss.

Le Grand ([27]) argues that ISRM tends to focus on threats without considering opportunities, which in brief means taking account of what can go wrong more than the benefits of information security. Therefore, they propose to shift the focus to opportunities to ensure that information security enables businesses to use new technology that keeps them innovative, while maintaining their competitive edge. Olsson ([29]) found empirical evidence showing that current information security risk management methodologies focus solely on negative risk, and that the absence of opportunity management is obvious, which is the same conclusion as from research conducted by Rajbhandari ([28]). Many years after the research conducted by Olsson ([29]) and Rajbhandari ([28]), the practice of assessing positive risk regarding information security has not gained much traction, even though the latest edition of ISO/IEC 27005:2022 ([7]) opens up for positive risk. This is also true for ISO 31010:2019 ([26]), which is a general guideline on risk assessment that focuses entirely on threats, with some mention of opportunities.

Our investigation found that there is limited research on assessment of positive risk. One of the few cases we have identified was by Ivascu and Cioca ([31]), who propose a risk model that consists of three components: the first component is to treat positive risk as opportunity management, the second component is to treat negative risk as hazard management, and the third component is control management, which is used to manage uncertainty. They also propose a model for risk treatment strategies specifically for opportunity, which was the inverse of the traditional risk treatment strategies. Hillson ([30]) argues that opportunities and threats do not differ, since both involve uncertainty, which affects the ability to achieve objectives. Hillson then proposed a double probability impact matrix for assessing opportunities and threats, and risk strategies similar to those of Ivascu and Cioca ([31]).

2.2 Research questions

This study aims to answer the following three research questions. First, how should practitioners interpret the concept of risk as defined in ISO/IEC 27005:2022 ([7]) to make it more applicable to both positive and negative risks? Second, how should a definition of positive risk be articulated? Finally, how can the definition of risk be applied to describe and assess both positive and negative risks?

3 Research method

This research started with a systematic literature review (SLR) procedure developed by Kitchenham [1]. However, by analysing the research data collected, we identified that there is limited research of positive risk and there was a need to choose a more appropriate research method. To answer the research questions, we needed to generate new theory due to limited research, but also manage our

predetermined ideas and biases, because these issues have been identified from our practical experience. To address these issues, we found that grounded theory (GT) is an appropriate research method for this project. The aim of GT is to gain an understanding of the data and to use this knowledge to construct new theory, which means that this research method is appropriate when little is known about a research phenomenon. While constructing theory founded on the data, we can better manage our predetermined ideas and biases. There are many variations of GT, but we choose to combine different variations based on a framework described by Chun Tie et al. [38], together with the main characteristics and guidelines described by Stol et al. [39] and Birks et al. [40], to match our research issues.

Our research started with SLR, but evolved over to GT, and to collect research data, we used purposive sampling from GT (Chun Tie, et al., [38]). The aim of purposive sampling is to select relevant data before further analysis. We decided that the most relevant digital libraries from which to collect research data were Web of Science, Scopus and Google Scholar because they cover a wide spectrum of research related to information security and risk management. However, due to limited research on this topic, we decided to collect relevant standards that are considered “best practice” by the industry, as well as mainstream textbooks used for industry certification programs, to understand how the industry applies risk management.

We then defined appropriate search keywords for a literature search. Our keywords consisted of strings that we considered relevant to the fields of study, as shown in the left-hand column of Table 1. We started with keywords related to information security, but surprisingly, there are limited papers discussing positive risks related to information security. We therefore decided to broaden the search by removing information security, with the intention of obtaining more papers related to positive risk. We decided not to collect papers from Google Scholar concerning the search string “Information Security Risk Management” because we encountered duplicate articles from other sources and found many entries other than research papers.

Table 1. Overview of relevant papers from research databases.

| Search keywords | Web of Science | Scopus | Google Scholar |
|--|----------------|--------|----------------|
| “Information Security Risk Management” | 13 | 16 | 0 |
| “Positive Risk Information Security” | 3 | 3 | 1 |
| “Opportunity Management” | 3 | 6 | 1 |
| “Positive Risk Management” | 1 | 1 | 1 |
| “ISO3100 Positive Risk” | 2 | 4 | 1 |

We then applied constant comparison, which is used to analyse data from different viewpoints and help researchers understand their data and the gaps in their data, to generate new theory (Birks, et al., [40]). By constantly comparing data, we can use this for coding and categorisation, to generate more

codes and different categories. Constant comparative analysis helps us find differences and consistencies/inconsistencies, to help us refine our theories or raise our understanding (Chun Tie, et al., [38]). The constant comparison helps us to collect data based on theoretical sampling, which constitutes collecting data to enrich the emerging theory or concepts until we reach theoretical saturation, when data ceases to give us new insight and we can predict what the analysis of the data is likely to describe (Birks, et al., [40]). In a way, this functions as constantly evolving inclusion and exclusion criteria similar to SLR, but in GT it is called theoretical sensitivity, which is knowing which theory is important to our own theory. We used an ever-evolving coding system as inclusion and exclusion criteria until we reached the point of theoretical saturation (Chun Tie et al., [38]).

Stol et al. [39] describe coding as an analytical method to label data according to its properties. The coding concepts we used were initial coding, core category and axial coding. At the initial coding level, the labels/codes are not categorised, but the main focus is to generate many codes, to give us an overview of the collected data. From the initial coding, we can then determine core concepts and use this data to generalise and categorise codes and then transfer the codes to respective categories. The final phase of coding is axial coding, of which the goal is to present interrelated codes or categories and explain relationships between the data, to ensure a better understanding of the data. To analyse and identify the interrelation between the codes and categories, we used diagramming tools to help us visualise and illustrate the complex interplay between codes and core categories (Mills, et al., [2]). The diagramming tool we used was Obsidian, which we used to develop codes, and then transferred the codes to their respective categories. Each code and category was marked and labelled with our interpretations and restructured to match similar codes. Obsidian can then illustrate how the codes are interrelated and give us a better overview, to generate more theory or collect more data to repeat this research process.

This resulted in 23 papers, and 32 codes are relevant for this study. The core categories are Industry standards (9 codes), Integration of RM (7 codes), Positive risk (2 codes), Risk challenge (5 codes), Risk communication (3 codes) and Standard risk (6 codes).

4 Results

Based on our research method, we observed two important findings. The first finding is related to the fundamental aspects of positive risk that need to be discussed and starts at a definition level. The second finding is that, to the best of our knowledge, there is limited research of how to conduct risk assessments of positive risk. These findings are described in separate subsections below.

4.1 Definition of risk

Before we can propose a definition for positive risk, we need to address the limitations of the current risk definition from ISO/IEC 27005:2022 ([7]) and

ISO 31000:2018 ([5]) to ensure consistency with these definitions. ISO/IEC 27005:2022 ([7]) and ISO 31000:2018 ([5]) state that risk is “*the effect of uncertainty on objectives*”, while the effect is a positive or negative deviation from the expected. The standards also described a note supporting the main definition that “*risk is usually expressed in terms of risk sources, potential events and their consequences and their likelihood*” (ISO 31000:2018, [5]). Our first observation is that the general definition of risk is too abstract for it to be applicable to describing information security risk. A similar statement is issued by Aven ([33]), who disagrees with the definition of risk from ISO 31000:2018 ([5]), arguing that it is inconsistent with the definition of “risk description” as “*Structured statement of risk usually containing four elements: sources, events, causes and consequences*”, where the uncertainty dimension is absent, and that to apply these elements, a risk analysis must first be conducted. We agree with Aven ([33]) to some degree, in the sense that describing all the elements generates too much information, because an important aspect of describing risk is to communicate risk simply to a recipient who is not necessarily an ISRM expert. This means that a risk description statement should be short, precise, easy to understand and tailored to the recipient.

The second limitation of the risk definition becomes evident on observing that risk can be identified from either a bottom-up or top-down approach (ISO 31010:2019, [12]). In our understanding, Aven ([33]) refers to a bottom-up approach and argues that a risk analysis is needed to include consequences and causes. We argue that it is possible to identify and describe risk first, then assess risk, and then refine the risk description afterwards, which is a top-down approach, and that both approaches have their pros and cons. To be clear, we could not find the definition of risk description in the new ISO 31000:2018 ([5]), ISO 31010:2019 ([12]) or ISO 27005:2022 ([7]). However, it still exists in *ISO Guide 73:2009 Risk management — Vocabulary* ([10]), but the issue remains because the definition is abstract and less applicable.

Our observation is that the main definitions from ISO 31000:2018 ([5]) and ISO/IEC 27005:2022 ([7]) are correct, depending on the stage of risk management that is applied. If risk management has not been applied, it makes sense to use the general definition, since it is abstract. This is similar to saying that uncertainty is classified in different categories, and Olsson ([29]) describes uncertainties as either aleatoric or epistemic. We argue that the general risk definition assumes aleatoric uncertainty whereby incidents cannot be foreseen in advance and could be random, so that the outcome could deviate from the expected. This is because when risk management has not been applied, risk is left to random outcomes and is unmanaged. In the next stage, when risk management has been applied, it makes more sense from a professional perspective to use a supplementary note on risk from ISO/IEC 27005:2022 ([7]), which states in brief that ISR is associated with potential threats that will exploit vulnerabilities which could cause harm to an organisation. Risk from a professional setting is like epistemic uncertainty, which derives from the lack of knowledge, where the goal is to

precisely understand the knowledge gap, to be able to seek more knowledge to foresee risk and manage it so that the outcome is less random.

However, the risk analyst should focus on understanding the epistemic uncertainty and how to manage it, while acknowledging the aleatoric uncertainty in the sense that not all risk can be foreseen. The goal is to manage both types of uncertainty of risk to an appropriate level. Based on this, we recommend that ISO standards clarify the distinct differences in the general and professional definition of risk. These notes from ISO/IEC 27005:2022 ([7]) can be used as a professional definition of risk and are practical. However, the notes are limited to negative risk and are inconsistent with the new definition. We will discuss five limitations of the current definition and propose an updated definition.

First, by saying “potential threats”, the note implies that ISR is limited to negative events. We propose to use “events” instead of “threats”, as both threat and opportunity are types of events. Second, the term “exploit” implies that an active entity is exploiting a vulnerability intentionally. Using “exploit” limits ISR to intentional exploiting and excludes accidental incidents or natural occurrences. Both unintentional incidents and natural occurrences affect information security objectives and we recommend removing “exploiting” from the note.

Third, the use of vulnerability makes sense when discussing technological risk. We argue that vulnerability is one of many causes, such as people or the process, and technological, economic and natural factors. It makes more sense to use “causes” instead of “vulnerabilities”, where the term “cause” is equally relevant for both positive and negative risks. Fourth, the last phrase of the definition: “*cause harm to an organisation*”, should be changed to “could affect business objectives”, since the goal of information security is to support business objectives and opens up for positive risk.

Finally, the general definition of risk implies that only the effect of uncertainty could be either positive or negative, which is the outcome. We argue that not only can the outcome be positive or negative, but the event itself can be framed as opportunity and/or threat, where the outcome could be either positive or negative. Based on these findings, we propose a supportive ISR definition to ISO/IEC 27005:2022 ([7]):

Definition 1. *“An information security risk is a possible security-related event that could affect business objectives.”*

The first part of the definition emphasises “a possible event” since the event could materialise or not, which is why a likelihood assessment is needed. The second part of the definition is related to consequence in the sense that if the event materialises, then business objectives can be affected positively or negatively. The other benefit of this definition is that it can be used as a template for describing the risk discussed in section 4.2. Now that we have defined general risk, which considers positive and negative risk, we can define positive risk as follows:

Definition 2. “A positive information security risk is a possible security-related opportunity that could help businesses achieve their business objectives.”

We define opportunity as a type of event that is positive, such as process improvement, acquisition, upgrading, patching and building competence. The aim is to identify security-related opportunities to provide value or improve an organisation. We deliberately added “possible” before opportunity because we do not know whether the opportunity will materialise. If it does materialise, this will depend on whether implemented controls increase the likelihood of the opportunity materialising. The last phrase of the definition is related to the gains the identified opportunity could support in terms of how an organisation achieves its business objectives, such as increased income, reputation, optimised service and reduced workload. We have deliberately added “could” to the last part of the definition, since an opportunity could fail if it were not managed well, which means that positive risk should be managed.

4.2 Risk description

By applying the proposed definition 1, it is possible to identify a possible event and outcome if the event materializes. The general template for describing a risk is as follows: *There is a possibility that <insert event> could result in <insert outcome>*. By assuming the possibility of an event as a threat/opportunity with a gain/loss as outcome, this template opens four ways to describe risk, as provided in Table 2. The aim of risk description strategies is to open up opportunities to apply risk framing, which is to communicate risk that is tailor-made for a specific recipient (Wangen and Snekkenes, [34]), since every recipient perceives risk differently, also known as risk perception (Lion and Meertens, [35]). Some decision-makers prefer positive information, while others can make effective decisions with negative information. Understanding the others’ risk perception can help a risk analyst frame risk in a way that suits the recipient. Using the risk description strategies gives access to four alternative ways of communicating and describing risk, as shown in Table 2. In contrast to traditional ISRM, which only provides the first alternative.

Table 2. Risk description strategies.

| Alternative | Risk description alternatives |
|-------------|--|
| 1. | There is a possibility that <insert threat> could result in <insert loss> |
| 2. | There is a possibility that <insert threat> could result in <insert gain> |
| 3. | There is a possibility that <insert opportunity> could result in <insert loss> |
| 4. | There is a possibility that <insert opportunity> could result in <insert gain> |

A use case on the practical use of risk description strategies is provided in section 4.3.

4.3 Sample case - Use of risk description strategies

The setting for this fictive case is a local private hospital that specialises in emergency healthcare. Medical doctors rely on advanced technology to perform emergency healthcare procedures. The top-level management has hired a risk analyst to perform a risk assessment because the technical system has been disrupted on several occasions, which has caused extensive loss of income and reputation. These disruptions have not impacted the patients, but top-level management is concerned about this scenario. Therefore, they require a risk assessment to determine whether to improve the system or acquire a new system. The risk analyst reviews the technical documentation and architecture description, and performs vulnerability scanning. The risk analyst also interviews key stakeholders, including the system owner, IT manager, top-level management and information security manager. The system owner wants to use the same system as before because they are accustomed to it, and the same applies to the IT manager, while only the information security manager wants a more robust system. The top-level management wants a solution that balances the needs of stakeholders, but also increases effectiveness and efficiency and provides a positive return on investment. From the interviews, the risk analyst has an idea of the stakeholders' risk perception.

The main findings are that the system is installed locally on different clients and servers spread across the hospital. There is no monitoring of the system, so the IT or security staff cannot detect potential incidents. When an incident occurs, the IT or security staff must be on-site to troubleshoot and fix the problem. It takes around 30 minutes for them to be on-site. Depending on the type of incident, it could take from one hour and up to two days to fix the issue. From these findings, the risk analyst concludes that there is a need for a centralised architecture with monitoring capabilities that could eliminate travel time, since IT and security staff would be able to troubleshoot offsite and fix problems before they occur, based on monitoring. The analyst's aim is to recommend the implementation of centralised architecture and monitoring capabilities. Since the risk analyst has mapped stakeholder risk perceptions, the analyst can use risk description strategies to match the different risk perceptions. The aim is to catch the stakeholders' attention and address their key concerns, so as to increase the likelihood of them listening to the assessment. The risk description serves as the first and fundamental line to catch the stakeholders' attention before presenting the assessment. In Table 3, we give examples of all four possibilities of framing risks based on strategies from Table 2, which will be discussed.

Alternative 1 from Table 3: *"There is a possibility that malware can be installed without detection, which could cause business disruption."* According to the risk description strategies provided in Table 2, the threat is that "malware can be installed" while the loss is related to "business disruption". Alternative 1 is suitable to communicate risk to security staff and top-level management. The security staff are accustomed to this rhetoric, since this is the traditional way of communicating risk from a threat-based approach. The top-level management might be interested in this approach because they care about the reputation of

Table 3. Practical use of risk description strategies.

| Examples |
|---|
| 1. There is a possibility that malware can be installed without detection, which could cause business disruption |
| 2. There is a possibility that malware can be installed without detection, which would not cause any business disruption |
| 3. There is a possibility that acquiring updated infrastructure (centralised, monitoring capabilities) could cause business disruption |
| 4. There is a possibility that by acquiring updated infrastructure detection of faults in the system (centralised, monitoring capabilities) could reduce the workload of the IT and security staff, and give a more reliable system |

the hospital. However, this will depend on the person, since some might prefer solution-based rhetoric. Therefore, in this case, we know that malware cannot be detected, and at some point, malware can be installed, since this is a common attack vector. This could cause business disruption and it could take time to troubleshoot the issue, because the staff need to travel to the physical location. In this case, there is a high probability of not detecting malware, and the consequences can be high because this could affect patient safety.

Alternative 2 from Table 3: *"There is a possibility that malware can be installed without detection, which would not cause any business disruption."* According to the risk description strategies provided in Table 2, the threat is that "malware can be installed", while the gain is that, even though the threat materialised, it did not cause business disruption and revenue can still be generated. Alternative 2 is suitable for communication with the IT and security staff. By assuming that the IT and security staff can address the issue, they will probably receive praise for the way they handle the situation. This might increase the likelihood of them listening to the risk assessment, but if we frame the risk negatively, then the staff might feel humiliated and fail to support the risk assessment. Therefore, in this case, the malware cannot be detected, as in alternative 1, but the consequence assessment can be adjusted to the middle of the consequence scale. Here, we can acknowledge that IT and security staff can handle the situation, but that it can be handled better with appropriate tools.

Alternative 3 from Table 3: *"There is a possibility that acquiring updated infrastructure (centralised, monitoring capabilities) could cause business disruption."* According to the risk description strategies provided in Table 2, the opportunity is "updating the infrastructure", which could lead to loss related to "business disruption". Alternative 3 is suitable for top-level management and when the decision is made to acquire the new infrastructure. Successful acquisition does not equal a successful outcome because it depends on managing opportunities such as staff building, training and sufficient resources.

Alternative 4 from Table 3: *"There is a possibility that acquiring updated infrastructure detection of faults in the system(centralised, monitoring capabilities) could reduce the workload of the IT and security staff, and give a more reliable system."* According to the risk description strategies provided in Table

2, the opportunity is “updating the infrastructure”, which gives rise to the gain that personnel’s workload is reduced and a more reliable system can generate more income than an unstable system. Alternative 4 is suitable for all stakeholders, and especially those who prefer solution-based rhetoric. In this case, we emphasise improving the infrastructure so that it can detect faults. The IT and security staff can thereby fix a problem before it becomes an incident. We use infrastructure instead of system because it is easier for non-technicians to understand that changes do not affect the functionality of performing emergency healthcare procedures and that reduced workload is in the interest of all stakeholders. Therefore, communication based on alternative 4 will address everyone’s concerns and support the overall goal of top-level management, which is to increase effectiveness, efficiency and return on investment. To address the return on investment, we develop measures or key performance indicators (KPI) related to every problem that is fixed before it becomes an incident, compared with the downtime before acquiring the system, and so on. It is easier to define measures with positive risk, while if we use alternative 1, we need to develop measures and KPIs related to malware attacks, and it is uncertain whether this specific scenario would occur enough to contribute a positive return on investment. Therefore, in this risk assessment, we need to address the measures needed to ensure successful acquisition and gain.

After the risk assessments are presented, the risk analyst recommends the acquisition of monitoring capabilities. The risk analyst presents an assessment of cost and benefit, return on security investment, and total cost of ownership, and concludes that the acquisition would most likely reach break-even. This means that this acquisition will generate neither profit nor loss; and therefore, if a malware attack occurs and the new system can detect and correct the incident without causing business disruption, technically the hospital will still not generate income directly.

However, the risk analyst recommends developing strategies to build business presence to improve business reputation and trust, which could indirectly generate more customers due to good information security, which in turn could generate income. The risk analyst gives an example where a hospital can handle a malware attack without business disruption, and then they need to go public and share lessons learned, which is one way of improving business reputation to show that this hospital has robust healthcare services. This could generate more interest and increase the likelihood of gaining more customers, which in turn could generate more income. The risk analyst presents a decision tree and possible scenarios of outcomes, depending on which decision is made, as shown in Figure 1.

The best possible positive risk is not implementing the monitoring capabilities and where no malware attack occurs, but if an attack does occur, the likelihood of handling the incident without business disruption is low. It is naturally possible that the incident can be handled well, even without monitoring capabilities. The best possible positive risk when implementing the monitoring capabilities is that if a malware attack occurs and it causes no business dis-

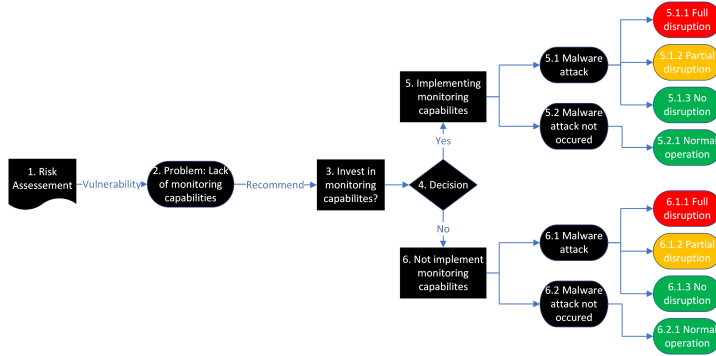


Fig. 1. Decision tree with possible outcomes

ruption, the hospital can employ strategies to increase its business presence to build its reputation, which could lead to more customers in the future. Another positive risk is if a malware attack has not occurred, then it is important to emphasise that monitoring could provide other non-economic gains, such as reduced workload and increased quality of their business services, which in turn could increase reputation and gain more customers.

This case presents different strategies to communicate risk based on recipients’ risk perception, and in this case the goal was to propose a solution, but communicated as four different strategies, instead of being dependent on the traditional way, which is alternative 1, the threat-based approach.

4.4 Positive risk assessment

Before we can conduct a positive risk assessment, it is beneficial to have an idea of how these aspects fit the proposed definition from section 4.1. Ivascu and Cioca ([31]) proposed a model for risk management that consists of three components: Hazard, Opportunity and Control Management. We will use this model as a basis and make some adjustments so that it fits into an ISRM context.

The use of hazard management focuses on negative events that could jeopardise business objectives. Hazard is not a familiar term used by information security professionals, and we recommend using threat because it is an established term in the information security community. Opportunity management is something we could keep, but we recommend that threat and opportunity are different types of events. We recommend adding a new component, objective, since it relates to consequences when a threat or opportunity is materialised, and the outcome could result in a loss or gain that affects the objective.

At the same time, we recommend removing control management because Ivascu and Cioca ([31]) consider this component to manage uncertainty that

affects the outcome of the risk. We find it more logical to lift uncertainty as a component that surrounds both the event and the objective. This is also to emphasise that managing uncertainty is not only about the outcome, but also about managing events as well and is not limited to the outcome. It seems that the ISO/IEC 27005:2022 ([7]) definition can be interpreted to mean that just the outcome can be positive or negative, and we argue that uncertainty management also applies to assessing the likelihood of the event. The updated conceptualisation of risk is presented in Figure 2.

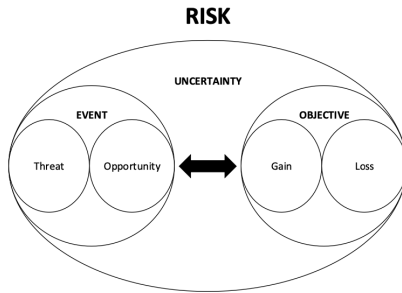


Fig. 2. Conceptualization of risk

Hillson ([30]) proposed a model for the double probability-impact matrix used for assessing opportunities and threats. The purpose of this matrix is to help professionals visualise and reflect on positive and negative risks. From this matrix, we propose some adjustments to fit our risk definition and description strategies. We propose to use likelihood instead of probability, since this is used in ISO/IEC 27005:2022 ([7]), and then we propose to use loss and gain instead of positive or negative impact. It makes more sense to determine a gain value instead of using positive impact. For instance, it is more intuitive to communicate a very high gain instead of a very high positive impact. The original model from Hillson ([30]) is a two-dimensional risk matrix, which we modified into a four-dimensional model so that it matches the four risk description strategies as provided in Table 2. The four-dimensional risk matrix model is presented in Figure 3.

5 Summary and Conclusion

The aim of the present study has been to extend the understanding of positive risk in the context of information security. In particular, this paper proposes a business oriented definition of information security and positive risk that is

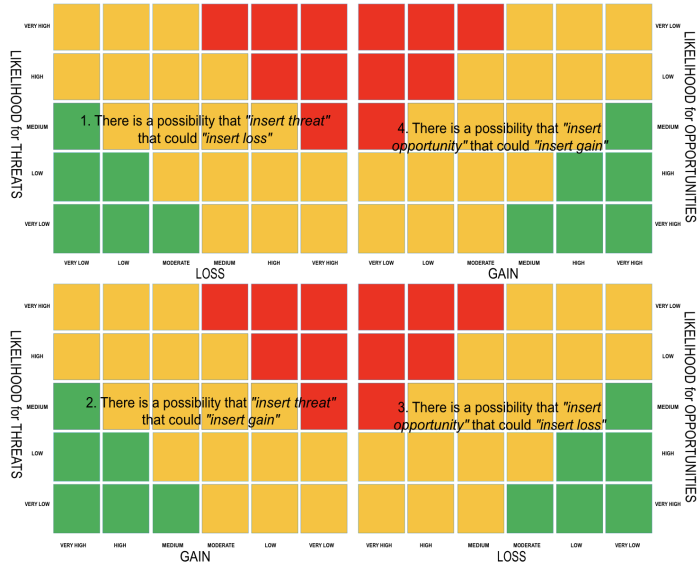


Fig. 3. Four-dimensional risk matrix

applicable to describe risk. A strategy to describe and frame risk in four different ways then depends on the risk perception of decision-makers. Finally, we propose conceptual models for the information security risk definition, as a four-dimensional risk assessment matrix tailored for this study. To the best of our knowledge, this is the first study to propose strategies for risk description with a corresponding risk matrix to assess both positive and negative risks. Further research should be conducted to validate these concepts, and this could be done by applying these concepts in a professional business setting and then conducting interviews with security professionals to learn more about their experience. Even though this study offers a theoretical contribution, it still provides ideas on assessing positive risk and can give researchers and professionals ideas to reflect on threats and opportunities. Based on ISO 31000 ([5]) that since 2009 have incorporated positive risk, as well as on the recent ISO/IEC 27005:2022 ([7]), it is reasonable to assume that steering committees, stakeholders and business leaders will expect information security professionals to identify and assess positive information security risk opportunities. Since the risk management field is evolving, information security professionals should adapt to this change, which could also help them get a more holistic perspective in information security and speak the same language as management (Tran and Jøsang, [41]).

References

1. Kitchenham, B.: Procedures for performing systematic reviews. Keele, UK, Keele University, 33(2004), 1–26 (2004)
2. Mills, J., Bonner, A. & Francis, K. The development of constructivist grounded theory. *International Journal Of Qualitative Methods*. **5**, 25-35 (2006)
3. Whitten, D. The chief information security officer: An analysis of the skills required for success. *Journal Of Computer Information Systems*. **48**, 15-19 (2008)
4. Standardization, I. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. (2022)
5. Standardization, I. Risk management — Guidelines. (2018)
6. Standardization, I. Information technology — Security techniques — Information security management systems — Overview and vocabulary. (2018)
7. Standardization, I. Information security, cybersecurity and privacy protection — Guidance on managing information security risks. (2022)
8. Standardization, I. Quality management systems — Requirements. (2015)
9. International Organization for Standardization - 0.Explanatory note and overview on ISO Survey 2021 results, = <https://www.iso.org/the-iso-survey.html>. Last accessed 13 Jan 2023
10. Standardization, I. ISO Guide 73:2009, Risk management — Vocabulary. (2009)
11. Standards, T. & Technology Risk Management Framework for Information Systems and Organizations. (2018), = <https://doi.org/10.6028/NIST.SP.800-37r2>. Last accessed 13 Jan 2023
12. Standardization, I. Risk management - Risk assessment techniques. (2019)
13. Harris, S. & Maymi, F. CISSP All-in-One Exam Guide, Seventh Edition. (McGraw Hill LLC,2016)
14. Gregory, P. CISM Certified Information Security Manager All-in-One Exam Guide. (McGraw Hill LLC,2018)
15. Standardization, I. Information security, cybersecurity and privacy protection — Guidance on managing information security risks. (2018)
16. Mayer, N., Aubert, J., Grandry, E., Feltus, C., Goettelmann, E., Wieringa, R. An integrated conceptual model for information system security risk management supported by enterprise architecture management. *Software & Systems Modeling*. **18**, 2285-2312 (2019)
17. Bergström, E., Lundgren, M. & Ericson, R. Revisiting information security risk management challenges: a practice perspective. *Information & Computer Security*. (2019)
18. Diefenbach, T., Lucke, C. & Lechner, U. Towards an Integration of Information Security Management, Risk Management and Enterprise Architecture Management—A Literature Review. *2019 IEEE International Conference On Cloud Computing Technology And Science (CloudCom)*. pp. 326-333 (2019)
19. Abbass, W., Baina, A. & Bellafkih, M. Improvement of information system security risk management. *2016 4th IEEE International Colloquium On Information Science And Technology (CiSt)*. pp. 182-187 (2016)
20. Fenz, S., Heurix, J., Neubauer, T. & Pechstein, F. Current challenges in information security risk management. *Information Management & Computer Security*. (2014)
21. Tran, D. & Jøsang, A. Information Security Posture to Organize and Communicate the Information Security Governance Program. *Proceedings of the 18th European Conference On Management Leadership And Governance, ECMLG 2022*. **18**, 515–522 (2022)

22. Aleksandrov, M., Vasiliev, V. & Aleksandrova, S. Implementation of the Risk-based Approach Methodology in Information Security Management Systems. *2021 International Conference On Quality Management, Transport And Information Security, Information Technologies (IT&QM&IS)*. pp. 137-139 (2021)
23. Shamala, P., Ahmad, R., Zolait, A. & Sedek, M. Integrating information quality dimensions into information security risk management (ISRM). *Journal Of Information Security And Applications*. **36** pp. 1-10 (2017)
24. Webb, J., Ahmad, A., Maynard, S. & Shanks, G. A situation awareness model for information security risk management. *Computers & Security*. **44** pp. 1-15 (2014)
25. Riesco, R. & Villagr a, V. Leveraging cyber threat intelligence for a dynamic risk framework. *International Journal Of Information Security*. **18**, 715-739 (2019)
26. Putra, I. & Mutijarsa, K. Designing Information Security Risk Management on Bali Regional Police Command Center Based on ISO 27005. *2021 3rd East Indonesia Conference On Computer And Information Technology (EIConCIT)*. pp. 14-19 (2021)
27. Le Grand, C. Positive Security, Risk Management, and Compliance. *EDPACS*. **47**, 1-10 (2013)
28. Rajbhandari, L. Consideration of opportunity and human factor: required paradigm shift for information security risk management. *2013 European Intelligence And Security Informatics Conference*. pp. 147-150 (2013)
29. Olsson, R. In search of opportunity management: Is the risk management process enough?. *International Journal Of Project Management*. **25**, 745-752 (2007)
30. Hillson, D. Extending the risk process to manage opportunities. *International Journal Of Project Management*. **20**, 235-240 (2002)
31. Ivascu, L. & Cioca, L. Opportunity risk: integrated approach to risk management for creating enterprise opportunities. *Advances In Education Research*. **49**, 77-80 (2014)
32. Purdy, G. ISO 31000: 2009—setting a new standard for risk management. *Risk Analysis: An International Journal*. **30**, 881-886 (2010)
33. Aven, T. On the new ISO guide on risk management terminology. *Reliability Engineering & System Safety*. **96**, 719-726 (2011)
34. Wangen, G. & Snekenes, E. A taxonomy of challenges in information security risk management. *Proceeding Of Norwegian Information Security Conference/Norsk Informasjonssikkerhetskonferanse-NISK 2013-Stavanger, 18th-20th November 2013*. (2013)
35. Lion, R. & Meertens, R. Security or opportunity: the influence of risk-taking tendency on risk information preference. *Journal Of Risk Research*. **8**, 283-294 (2005)
36. Axelos. ITIL Foundation, ITIL (ITIL 4 Foundation). (The Stationery Office, 2020)
37. Measuring and Managing Information Risk: A FAIR Approach. (Butterworth-Heinemann, 2014)
38. Chun Tie, Y., Birks, M. & Francis, K. Grounded theory research: A design framework for novice researchers. *SAGE Open Medicine*. **7** pp. 2050312118822927 (2019)
39. Stol, K., Ralph, P. & Fitzgerald, B. Grounded theory in software engineering research: a critical review and guidelines. *Proceedings Of The 38th International Conference On Software Engineering*. pp. 120-131 (2016)
40. Birks, D., Fernandez, W., Levina, N. & Nasirin, S. Grounded theory method in information systems research: its nature, diversity and opportunities. *European Journal Of Information Systems*. **22**, 1-8 (2013)
41. Tran, D. & Josang, A. Business Language for Information Security. *International Symposium On Human Aspects Of Information Security And Assurance*. pp. 169-180 (2023)

Appendices

Appendix A

Appendix

A.1 Interview guide - Paper/book II

Intervjuguide – Informasjonssikkerhetsledelse

| Tema | Spørsmål |
|-----------------------|--|
| Introduksjon | 1. Hvilke ferdigheter mener du en ISL bør ha? (Åpen spørsmål) |
| Introduksjon | 2. Hvor lærte du disse ferdighetene? |
| Introduksjon | 3. Hva mener du er den viktigste jobben til en ISL? a. Kun en ting |
| Informasjonssikkerhet | 4. Hvilke informasjonssikkerhetsmessige fag mener du en ISL må kunne? |
| Informasjonssikkerhet | 5. Hvilke informasjonssikkerhetsmessige fagområder mener du en ISL må kunne på: a. Grunnleggende b. Viderekommende c. Fordypning d. Hvorfor? |
| Andre fagområder | 6. Hvilke <u>ikke</u> -informasjonssikkerhetsfaglige fag mener du en ISL bør ha? |
| | 7. Hvilket tankesett mener du en ISL bør ha? |
| Andre fagområder | 8. Hvilke områder innen ledelse er relevant for en informasjonssikkerhetsleder? |
| Personlig utvikling | 9. Hvilke personlige verdier mener du en ISL bør ha? |
| Personlig utvikling | 10. Hvordan praktisere den verdien du mener er viktigst? |
| Ledelse | 11. Hvordan snakker man forretningspråket? |
| Ledelse | 12. Hva kjennetegner forretningspråket? |
| Ledelse | 13. Noen tanker på hvorfor vi skal snakke forretningspråket? |
| Ledelse | 14. Hvilket tankesett bør man ha når man snakker forretningspråket? |

Appendix B

Co-Author declarations

B.1 Paper I

Co-author declaration for the following joint paper:

This declaration should describe the research contribution of the candidate, the main supervisor (where he/she is an associate author) and the other two most central authors (the corresponding author must be among them). If applicable, the contributions from other PhD candidates who has or intend to include the paper in a thesis should be described. Contributions from master students should be described.

Authors: Tran, Dinh Uy and Jøsang, Audun

Title: Information Security Posture to Organize and Communicate the Information Security Governance Program

Journal: *Proceedings*

of the 18th European Conference on Management Leadership and Governance. (2022), pp. 515–522. DOI: 10.34190/ecmlg.18.1.729.

Dinh Uy Tran's independent contribution:

First author Corresponding author Other

Design and Idea building, Writing the full first draft of the paper, quality check, finalizing paper and responding to reviewer comments.

Audun Jøsang

First author Main supervisor Corresponding author PhD candidate Other

Ideabuilding, edits, proofreading and quality check

<Co-author's name>

First author Main supervisor Corresponding author PhD candidate Other

<Co-author's contribution>

x

First author Main supervisor Corresponding author PhD candidate Other

<Co-author's contribution>

Has this paper been, or will this paper be part of another doctoral degree thesis?

Yes: No:

If yes, elaborate:


Contributions from master students:




Do you verify that Dinh Uy Tran has contributed to this joint paper as described above?

Yes: No:

If no, specify:


.....
Dinh Uy Tran


.....
Audun Jøsang

signatures:

B.2 Paper III

Co-author declaration for the following joint paper:

This declaration should describe the research contribution of the candidate, the main supervisor (where he/she is an associate author) and the other two most central authors (the corresponding author must be among them). If applicable, the contributions from other PhD candidates who has or intend to include the paper in a thesis should be described. Contributions from master students should be described.

Authors: Tran, Dinh Uy and Jøsang, Audun

Title: Business Language for Information Security

Journal: *Furnell, S., Clarke, N. (eds) Human Aspects of Information Security and Assurance. HAISA 2023. IFIP Advances in Information and Communication Technology, vol 674. Springer, Cham., pp. 57–68. DOI: 10.1007/978-3-031-38530-8_14.*

Dinh Uy Tran's independent contribution:

First author Corresponding author Other

Design and Idea building, Writing the full first draft of the paper, quality check, finalizing paper and responding to reviewer comments.

Audun Jøsang

First author Main supervisor Corresponding author PhD candidate Other

Ideabuilding, edits, proofreading and quality check

<Co-author's name>

First author Main supervisor Corresponding author PhD candidate Other

<Co-author's contribution>

x

First author Main supervisor Corresponding author PhD candidate Other

<Co-author's contribution>

Has this paper been, or will this paper be part of another doctoral degree thesis?

Yes: No:

If yes, elaborate:

Contributions from master students:



Do you verify that Dinh Uy Tran has contributed to this joint paper as described above?

Yes: No:

If no, specify:

[signature removed]

Dinh Uy Tran

Audun Jøsang

.....

B.3 Paper IV

Co-author declaration for the following joint paper:

This declaration should describe the research contribution of the candidate, the main supervisor (where he/she is an associate author) and the other two most central authors (the corresponding author must be among them). If applicable, the contributions from other PhD candidates who has or intend to include the paper in a thesis should be described. Contributions from master students should be described.

Authors: Tran, Dinh Uy, Sigrid Haug Selnes, Janne Hagen and Jøsang, Audun

Title: An Opportunity-Based Approach to Information

Security Risk

Journal: *The 4th International Workshop on Cyber-Physical Security for Critical Infrastructures Protection (CPS4CIP 2023).*

Dinh Uy Tran's independent contribution:

First author Corresponding author Other

Design and Idea building, Writing the full first draft of the paper, quality check, finalizing paper and responding to reviewer comments.

Sigrid Haug Selnes

First author Main supervisor Corresponding author PhD candidate Other
Risk management expertise, proofreading and quality check

Janne Hagen

First author Main supervisor Corresponding author PhD candidate Other
Idea building, quality check

Audun Jøsang

First author Main supervisor Corresponding author PhD candidate Other
Edits, proofreading and quality check

Has this paper been, or will this paper be part of another doctoral degree thesis?

Yes: No:

If yes, elaborate: Sigrid Haug Selnes is a PhD candidate and will use this paper as a part of her doctoral degree thesis.

Contributions from master students:



Do you verify that Dinh Uy Tran has contributed to this joint paper as described above?

Yes: No:

If no, specify:

[signature removed]

Dinh Uy Tran

Sigrid Selnes

Janne Hagen

Audun Jøsang