Kristiania
University
College

Master of Information Systems: Management and Innovation

Exploring Organisational ISMS Alignment with Structuration Theory: A Case Study in a Norwegian Public Sector Agency

Henrik Frellumstad Jenssen & 865219

A report submitted in partial fulfilment of the requirement for the degree of Master of Information Systems: Management and Innovation

Supervisor: Gebremariam Assres

Restricted: □ Yes ■ No

Kristiania University College
Prinsensgate 7-9
0107 Oslo
Norway

Abstract

Information Security Management Systems (ISMS) provides organisations with guidance and strategies on how to implement information security into their organisations and achieve resiliency. It is largely recognised that adequate information security resilience is achieved through people, processes, and technology. Despite this recognition, however, several organisations still struggle to achieve proper alignment of information security across the organisation. For many organisations, there is a misalignment between their information security and their overarching organisational objectives. This is often represented by perceptions that information security is a technical problem and is removed from the activities and processes which support the daily organisational objectives. This misalignment can create situations where the ISMS of an organisation is not enacted properly. This research has set out with the purpose of elucidating how these misalignments occur and suggest possible opportunities for alignment. This sought is achieved through the use of Anthony Gidden's structuration theory, which Wanda Orliwkoski has put into a theoretical framework which can be applied to empirical conditions. This framework has allowed this thesis to approach ISMS alignment in a novel and theoretical way, by identifying recursive structures which inform organisational activities and processes. This has been done at a Norwegian public sector agency. This led the research to identify structures within the organisational setting which pose obstacles to the necessary ISMS alignment. Simultaneously it identified structures which provide opportunities for the ISMS to align itself with existing activities and processes. This research, thus, provides one practical and one theoretical result. Firstly, it has diagnosed organisational reasons as to why the ISMS at the agency has not been integrated in a desired manner. Secondly, it has demonstrated the explanatory power of the theoretical framework, thus providing information security researchers a new tool to study and analyse ISMS alignment with.

Keywords: ISMS, information security, information security culture, information security governance, strategic and organisational alignment, structuration theory, Action Design Research

Acknowledgements

The list of people who have helped me throughout the research and writing process is long, and I would not be able to mention them all. However, I would in particular like to thank my supervisor, Dr. Gebremariam Assres for his help, guidance and advice. I would also like to thank Dr. Lester Lasrado and Dr. Miria Grisot for volunteering to provide me with guidance.

Moreover, I am also exceptionally grateful to everyone at NorAg. Their support and willingness to help made this research possible. I am also especially appreciative to everyone who took time out of their busy days to let themselves be interviewed. Their willingness and interest to participate was fundamental in providing the necessary insights and analysis.

I certify that the work presented in the thesis is my own unless referenced

Signature:

Date: 23.05.2021

Total number of words: 20 822

Table of Contents

Table of Tables

Table of Figures

1. Introduction

Users have demonstrated an entrenched ability to use technologies and systems in ways which were unintended by inventors and designers (Orlikowski 2000) (Orlikowski and Yates 2006) (Kayworth and Whitten 2010). This can happen through error (lack of understanding, misalignment) or intent (inertia, subversion, omittance) (Orlikowski 2000). Yet no matter the way in which it has come about, the manner which users engage with technologies and systems tend to be affected by social practices and processes (Orlikowski 2000). This signifies that the functioning of technologies and systems cannot be analysed in and of itself, separated from the context in which it is intended. It must, instead, be considered and analysed in the social and organisational setting where it is implemented and integrated.

Information security can be considered a system which contain people, process and technology. There is therefore a distinctive human factor to information security. Organisational and individual practices, incentives, intentions and competence have been identified as vital factors in the alignment of an organisation's information security (Thomson, Von Solms. and Louw, 2006) (Vroom and Von Solms 2004) (Herath and Rao 2009) (Ifinedo 2012). This is considered so decisive that technical security controls of an organisation can be rendered ineffective if it is not accompanied by the correct socio-organisational alignment (Vroom and Von Solms 2004) (Thomson, Von Solms. and Louw, 2006) (Herath and Rao 2009) (Ifinedo 2012). Understanding how information security becomes embedded into the organisational activities and processes is therefore a pressing issue within information security, both in academia and in practice. This thesis seeks to contribute towards this area of inquiry.

1.1 Problem Description

Over the past years, upper management has come to realise that information security is not an optional addition, but a necessity (Knapp, Marshall, Rainer and Ford 2006) (Corriss 2010). Much of the awareness hails from the financial costs associated with information security events (Tweneboah-Kodua, Atsu and Buchanan 2018) (Yayla and Hu 2011). Consequently, the resources invested in organisational information security over the past decades have risen to significant sums (KPMG 2020) (Bissell, Lasalle and Cin 2020) (Bauer, Scherf, von der Tann and Klinkhammer 2017). Despite this, a large number of organisations still find their information security resilience to be inadequate (KPMG 2020) (Hall, Sarkani and Mazzuchi 2011) (Bissell, Lasalle and Cin. 2020) (Bauer, Scherf, von der Tann and Klinkhammer 2017). Research has, in fact, demonstrated that there are not necessarily correlations between increased spending and increased information security resilience (Bauer, Scherf, von der Tann and Klinkhammer 2017, pp. 8-12) (Van Niekerk and Von Solms 2006). Instead, the way towards increased information security resilience has been identified to exist within the intersection of 'people, processes, technology, and operations capabilities.' (Hall, Sarkani and Mazzuchi 2011, pp. 155-156) (Jackson and Rahman 2017, p. 44) (Da Veiga and Martins 2015). This intersection is linked to what is known as strategic alignment, which allows information security efforts to be integrated and understood as a part of the foundational, organisational activities, processes and objectives (KPMG 2020) (Bauer, Scherf, von der Tann and Klinkhammer 2017) (Jackson and Rahman 2017).

This form of alignment is multifaceted and comprehensive, but there are particularly two, notable and overarching barriers to this alignment. The first barrier is posed by information security itself. There is a tendency for information security to demonstrate an obsessive focus on the security in and of itself, making it appear misaligned with the organisation's overall objectives. (Whitman and Mattord 2011, p. 23) (Reece and Stahl 2015) (Jackson and Rahman 2017). For the vast majority of organisations information security is not an objective in itself, but an auxiliary function that ought to support their primary objectives (Jackson and Rahman 2017, p. 44) (Fitzgerald 2007, pp. 261-262) (Fredriksen 2017, pp. 83-84). These propensities can cause a schism between the propagators of information security on the one side, and the so called 'rest' of the organisation on the other. The second barrier is posed by the 'other' part of the organisation. There is a propensity for the 'normal' employees, those who are concerned with the everyday, organisational objectives, to not understand how the information security align with their daily activities and processes (Farahmand, Atallah and Spafford 2012). While information security is recognised as important to safeguard organisations and their information, there is a tendency to view information security as a challenge which is delimited to IT and security staff (Corriss 2010). Paradoxically, however, to achieve adequate information security resilience, it is recognised that information security measures must be understood and integrated into the everyday organisational activities, processes and objectives (Whitman and Mattord 2011, p. 24) (Kayworth and Whitten 2010) (Jackson and Rahman 2017) (Corriss 2010).

The alignment of information security into the daily activities and processes of employees is a part of what is known as 'information security culture.' An information security culture refers to a condition where normal employees internalise information security considerations into their everyday decision-making, activities and processes (Karlsson, Åström, and Karlsson 2015) (Knapp, Marshall, Rainer and Ford 2006) (Da Veiga and Martins 2015) (Corriss 2010).

Exactly how such a culture is created is still a topic of debate (Karlsson, Åström, and Karlsson 2015). One perspective emphasises management buy-in, which is considered an enabler for acceptance and support throughout the organisation (Da Veiga, and Martins 2017) (Straub and Welke 1998) (Hu, Dinev, Hart, and Cooke 2012) (Whitman and Mattord 2011, p. 24) (Kayworth and Whitten 2010) (Soomro, Shah and Ahmed 2016) (Jackson and Rahman 2017). There is, however, a general acceptance that information security must become integrated into the daily activities and processes of the employees (Knapp, Marshall, Rainer and Ford 2006) (Corriss 2010) (Martins and Elofe 2002) (Da Veiga and Eloff 2010) (Van Niekerk and Von Solms 2010) (Thomson, Von Solms. and Louw 2006).

It is within this context, the intersection between information security alignment and culture, that this thesis has situated itself. This indicates that the thesis has largely omitted the 'technology' dimension of information security, rather focusing on the 'process' and 'people' dimensions. While the thesis is situated within the two discourses mentioned above, the study does not seek to solidly belong to either one of them. The thesis has, instead, sought to take a more systems-orientated approach, where a focus has been put on understanding interconnecting aspects within the organisation (Meadows 2008, p. 14). This has been achieved through the utilisation of structuration theory, which seeks to explore the existing feedback loops between structure and agency. This inquiry has, therefore, sought to make connections across different concepts and literature within information security.

1.2 Thesis Context

This thesis has sought two, concrete contributions:

1) The first is a practical one. The author has been both an academic researcher and an employee in the organisation where the research has been conducted. The author participated in a project where the organisation in question sought to further augment its Information Security Management System (ISMS). This was considered the IT artefact which was the object of study. Because the author has had a dual role, the thesis has employed an Action Design Research (ADR) methodology. ADR is a methodology specifically shaped for research where the researcher is simultaneously involved in the project of study (Sein et al. 2011). The practical contribution sought has therefore been to analyse a concrete, organisational problem, and then suggest a possible, practical solution. This solution is intended to provide the organisation with a tangible suggestion on how to solve the problem. Moreover, although this problem is a case specific example, the issue of

information security alignment is a frequently recurring issues for a plethora of organisations. The aspiration has therefore also been for this study to provide insight for organisations with similar challenges.

2) Secondly, the thesis has sought to provide a theoretical contribution to the academic fields of Information Systems and Information Security. By doing this, the author is seeking to answer four calls.
    i. First, this is a response to the assertion that master students within Information Systems often fall short of providing a theoretical, and thus more generalisable, contribution towards the academic field (Presthus and Munkvold 2016).
    ii. Secondly, this is a response to the inquiries for the increased construction of methodological frameworks and theoretical foundations for the field of Cyber Security (Valeriano and Gomez 2020). This has been sought achieved primarily through the use of Anthony Giddens's structuration theory. An existing, theoretical framework explaining the process of structuration, created by Orlikowski (2000), has been repurposed to analyse the structuration of information security. By doing this, an endeavour has been made repurpose a well-recognised theoretical framework and apply it to a field in need of theoretical exploration and rigidity.
    iii. Thirdly, there has been calls for theory testing within studies on information security culture (Karlsson, Åström, and Karlsson 2015). Due to various limitations, this study has only been able to empirically apply the theory in one organisational case. Yet, this will still provide an insight into the viability of the theory.
    iv. Fourthly, as will be explored, the successful alignment of effective information security in an organisation is a prevalent challenge for most organisations. Consequently, it is also a focus in academia. Hence, testing a theoretical framework in this context can potentially open new avenues for academic inquiry.

1.3 Theoretical Context

The study has been conducted according to an interpretivist, epistemological paradigm. The thesis has utilised a theoretical framework based on structuration theory. Through this framework, the study has sought to categorise different forms of structures which operate within an organisation. By structures, it is meant that there are socio-organisational feedback loops which perpetuate certain recursive activities and processes. These social structures provide employees with an understanding of what organisational activities and processes are correct and purposeful, and which are not. In this thesis, information security is identified as its own form of structure. When information security is sought introduced into an organisation, through the ISMS, it indicates that it will encounter already existing structures. Because these existing structures embody the foundational activities and processes of the organisation, the information security structure might fail to align, and thereby fail to acquire the foothold it requires to become integrated into the organisation. When attempting to integrate information security across the organisation, it would therefore be necessary to identify and understand these structures.

1.4 Case Description

The thesis is a direct result of an information security initiative within a Norwegian state agency (henceforth referred to as NorAg). NorAg is primarily concerned with financing for the purpose of economic development in Norway. Its activities are broadly made up of financing and advisory services directed at bolstering Norwegian businesses. The organisation has between 500-999 employees and has about 45 offices in Norway and abroad. Although the organisation has a clearly defined organisational purpose, it is a comprehensive organisation with a wide range of activities. The organisation has its own IT department, with its own information security team. The organisation has been recognised for its digital maturity and rapid digital developments. Due to this, information security stands as a central focus within the organisation. Moreover, due to its financial responsibilities and its role as an important state agency, it has crucial social, economic, ethical and legal responsibilities to achieve a high level of information security resilience. The organisation is therefore continuously seeking to develop on its information security efforts.

The research for this thesis was initiated in the beginning of 2020, coinciding with a new information security project at NorAg. The project sought to complement the existing ISMS, based primarily on the ISO/IEC 27000 family, with the NIST CSF. The purpose would be to conduct a maturity assessment and enhance the information security resilience of the organisation. Focus was dedicated to ensuring that the assessments would provide tangible suggestions for improvement. This would be done through the cooperation between the in-house information security team and an external consultancy. The author took part in this project. After a discussion with the information security team, it was decided that the purpose of this thesis would be to inquire into how the ISMS is propagated outside the IT department. After some initial research, primarily based on the internal information security documents, the topic of this thesis was further narrowed down to exploring how the ISMS is, or is not, aligned with organisational activities and processes.

1.5 Thesis Objective

Organisations can be considered a collection of capabilities organised to achieve a certain purpose (Jackson and Rahman 2017, p. 44). Information security is therefore predominantly an auxiliary function of an organisation, rather than a main objective. Yet, despite their supportive essence, organisational leaders and management recognise that information security is a high priority for their organisation (Cisco Secure 2020). Despite these premises, however, many organisations suffer from inadequate information security resilience due to problems with integrating information security into their activities and processes. The purpose of this thesis has been to utilise a theoretical framework to explore potential explanations and solutions to this challenge.

This has been sought achieved through a theoretical framework based on structuration theory. Through this framework the thesis seeks to categorise different forms of structures which operate within an organisation. By structures, it is meant that there are socio-organisational feedback loops which perpetuate certain recursive activities and processes. These social structures provide employees with an understanding of what organisational activities and processes are correct and purposeful, and which are not. In this thesis, information security is identified as its own form of structure. When information security is sought introduced into an organisation, through the ISMS, this indicates that it will encounter already existing structures. Because these existing structures embody the foundational activities and processes of the organisation, the information security structure might fail to align, and thereby fail to acquire the foothold it requires to become integrated into the organisation. When attempting to integrate information security across the organisation, it would therefore be necessary to identify and understand these structures. In this pursuit, the thesis intends to answer two separate, yet highly interconnected, research questions:

RQ #1 How does the processes of structuration at NorAg affect the ISMS alignment across the organisation?

RQ #2 To what extent can a theoretical framework based on structuration theory elucidate possible problems with the alignment of information security across an organisation?

1.6 Brief Overview of the Chapters

Chapter 1 was dedicated to explaining the premise of the project and providing an insight into the various contexts which the project was situated within. Chapter 2 continues to build the context by providing an overview over related research. Most of the literature employed in this thesis has been taken from research on Information Security and Structuration Theory. In addition, there has been an emphasis put on literature discussing Action Research and Action Design Research. The methodology is covered extensively in Chapter 3, which is spent explaining the research methodology and the various concepts which has been used to complement the research. While the thesis has used Action Design Research as its overarching methodology, it has employed concepts from Action Research to complement the process. Chapter 4 presents the findings, consisting of five different structures which was identified in the research. In Chapter 5, each identified structure is analysed with the intention to uncover the significance of the findings. Chapter 6 is then spent highlighting and addressing some of the more pressing limitations of the research project. Chapter 7 is spent discussing the implications of the research both for the practical dimension of ISMS and the academic fields of Information Systems in general and Information Security in particular. Lastly, the thesis rounds up by highlighting how the research questions have been answered, and by providing suggestions to the case organisation based on the research.

2. Theoretical Framework and Related Research

2.1 Literature Overview

This thesis has largely drawn upon three independent strands of literature:

2.1.1 – #1 Information Security

The first is literature done on information security. This literature has had a twofold dimension. One part of the literature has been based on the academic scholarship done on information security, while the other has been based on the professional and practical literature. The former consists mostly of literature that addresses various aspects of Information Security, such as Information Security Management, Information Security Culture, and more. How the literature was discovered and selected will be presented below. The professional literature is primarily represented by consultancy reports by leading firms within the field of information security; publications, guidelines and research done by information security organisations; and literature written by professionals for professional application.

2.1.2 – #2 Structuration Theory

The second is literature done on structuration theory. This area can further be divided into two separate strands. The first is the original work done by Anthony Giddens, the creator of structuration theory. The second is the later work done on structuration work, primarily by scholars within Information Systems, which have sought to utilise structuration theory to better understand information technology in organisations. This has particularly been based on and inspired by the work done Wanda Orlikowski.

2.1.3 – #3 Action Research and Action Design Research

The third strand is literature done on Action Research and Action Design Research. The thesis has dedicated a significant amount of space to extensively explain its methodology. This was done for two specific reasons. Firstly, AR, and associated methodologies based on AR, are notably interpretive and situational (Checkland and Holwell 2007). Due to this, they can suffer from a lack of rigidity (Checkland and Holwell 2007, p. 5). It was, thus, essential that the methodology was constructed with sufficient academic integrity and rigidity. The second reason is because of the complementary relationship between AR (or in this case, ADR) and structuration theory. To ensure the academically proper use of AR, it is highly encouraged that it employs a theory which can provide the research with a theoretical framework (Checkland

1995) (Checkland and Holwell 2007) (McKay and Marshall 2007, pp. 144-147) (West and Stansfield 2001) (Oates 2005). This was thus sought achieved through the utilisation of structuration theory. This thesis also sought to incorporate McKay and Marshall (2007) distinction between the research methodology (M_R) and the problem-solving methodology (M_{PS}). Structuration theory has therefore contributed towards the creation of a problem-solving methodology (M_{PS}), which aids the researcher with assessing the organisational problem which is being sought addressed (McKay and Marshall 2007).

2.1.4 Literature Selection

With such comprehensive strands of literature being utilised, it was vital to seek guidance from sources of authority to ensure that the most appropriate and relevant literature was found. To achieve this, a number of different routes were taken:

1. First of all, academics at my educational institution, Kristiania University College, were approached and asked for guidance. The sources suggested were then used to engage in backwards referencing. The keywords used for the backwards referencing are provided in Table 2.1.
2. Secondly, the literature which was utilised in the course was reviewed for relevancy and utilised as a starting point for backwards referencing. In this endeavour, the classes on 'Introduction to Information Systems Research', 'IT Governance' and 'Information Risk and Security' provided notable direction. This review allowed for the identification of key scholars and pieces of literature. When such scholars were identified, Oria, the library search engine, and Google Scholar were utilised to identify more of their research. Keywords associated with the pertinent strand of literature were then searched for in association with the author. The keywords searched for are shown in Table 2.1. When additional literature by these scholars were found, the articles/chapters were indexed in order to keep an overview of their research.
3. Thirdly, literature reviews were used as efficient means to quickly get an overview of and become familiar with existing literature.
4. Lastly, as a general rule, the Senior Scholars' Basket of Journals, as provided by the Association for Information Systems, was considered the most optimal destination for literature on Information Systems and Information Security (AIS n.d.). When searching for literature with Oria, these journals were used as filters. However, because much of

the literature came from other academic fields, leading journals from these fields were also identified and utilised when relevant.

5. In addition, the professional literature on information security was also identified through recommendations and discussions with the information security team at NorAg.

Table 2.1 - Authors and Keywords

	Strands of literature		
Source	**Information Security**	**Theory / Structuration Theory**	**AR and ADR**
Academic staff	Coles-Kemp; von Solms.	Presthus and Munkvold.	Baskerville; Sein et al.; Hevner.
Course literature	Brotby.	Orlikowski.	Oates.
Backwards referencing	Whitman and Mattord; Da Veiga;	Giddens; Orlikowski and Robey; DeSanctis and Poole; Jones and Karsten; Mingers and Willcocks; Jones, Orlikowski and Munir; Walshm.	Checkland; Kock; Lee; McKay and Marshall.
Colleagues / work	NIST CSF; NIST SP 800-53; ISO 27001 and 27002; Ponemon Institute; Gartner.		
Literature reviews	Siponen; Soomro, Shah and Ahmed.	Orlikowski and Baroudi.	
Journals	Computers & Security; Information & Computer Security; Security and		

	Communication Networks;		
Keywords	Information Security Integration; Information Security Governance; Information Security Alignment; Information Security Culture; Organisational Capabilities; Information Security Management; Information Security Compliance.	Structuration Theory, Anthony Giddens; Information Systems Theories, Organizational Theories, Social Theory.	Action Research; Action Design Research; Soft Systems Methodology; Organisational Intervention; Interpretive Research.

Note: There were multiple instances where a scholar / literature was simultaneously derived at from the academic staff, from the course literature, and through backwards referencing. In these cases, the scholar has been placed where it was first discovered.

2.2 Information Security

Throughout the thesis, the word 'resilience' has been utilised to define a desirable end state for an organisation's information security. Although this definition remains fluid, information security resilience (also referred to as cyber security resilience) refers to a state where information security has become consolidated into the organisational strategy and the business continuity (Bissell, Lasalle and Cin 2020). This allows the organisation to dynamically achieve their organisational objectives with the appropriate amount of security preparedness and controls (Bissell, Lasalle and Cin 2020).

Furthermore, it must be acknowledged that there is an ongoing discourse about the exact meanings of information security on the one hand and cyber security on the other. It has yet to be established whether they can be used as synonyms or whether they define two different aspects of security (von Solms and van Niekerk 2013). For the purpose of this thesis, however, the two terms will be used as synonyms. There are two reasons for this. The first is that literature which discusses both information security and cyber security have been found highly relevant for the thesis. Hence, using only one of the terms was necessary to ensure conceptual clarity. Secondly, because of the organisational and practical focus of the thesis, the term which is used by the organisation in question has been opted for. This term is 'information security'. This is not to say that the debate on terminology is not an important one, it only signifies that it is outside of the scope of this thesis to participate in the debate. Additionally, throughout the thesis, the term *system* will often be mentioned. A system will be defined as the interconnected collection of parts which produce their own pattern of behaviour over time (Meadows 2008, p. 2). In the case of information security, this encompasses people, processes and technologies collected to safeguard information and value.

2.2.1 The CIA Triad

At the core of information security, one will find the CIA triad. The CIA triad embodies three, fundamental principles which lies at the heart of most information security efforts. These are:

- *Confidentiality*, the efforts to prevent unauthorised access to information (Stamp 2011, p. 2).
- *Integrity*, the efforts to prevent unauthorised alteration of information (Stamp 2011, p. 2).
- *Availability*, the efforts ensuring that information is available when needed (Stamp 2011, p. 2).

While these three principles can make information security seem somewhat uncomplicated, it does not make the topic an easy matter. The discourse contains elements of policy; management; governance; implementations; processes; technology; software; and hardware, to mention only some of the many dimensions belonging to information security (Solms 2006) (Coles-Kemp 2009) (Kayworth and Whitten 2010) (Stamp 2011) (Whitman and Mattord 2011) (Brotby 2009). All these dimensions can be discussed in depth, but in the name of simplification it can be said that these dimensions perform functions to:

- Protect an organisation's ability to function and achieve its goals;
- Protect the data and information collected and employed by an organisation;
- Enable the safe and reliable operation of the IT systems operated by an organisation;

- And safeguarding the technological assets of an organisation (Whitman and Mattord 2011, pp. 50-52).

This makes information security a sprawling and complicated field, and it is represented by everything from a 'No Access' sign on a fence to your typical hacker, attempting to unlawfully leverage exploits to breach an IT application. Due to the scope of field, it has therefore been necessary to narrow down the dimensions which are of most relevance for this thesis. Through this delimitation, this study has focused on the alignment of information security into NorAg, as specified by their Information Security Management System (ISMS). Through this delimitation, the study has had particular focus on information security as a management issue and as a governance issue (Soomro, Shah and Ahmed 2016) (von Solms 2006).

2.2.2 Information Security Governance

Lloyds of London has estimated that cyber-attacks cost businesses $400 billion globally each year (Hubbard and Seiersen 2016, p. 9). IBM and Ponemon Institute has estimated that the average cost of a breach is $3.92 million (IBM Security and Ponemon Institute 2019). Inevitably, the executive-level awareness of information security risk has increased drastically over the past year (Hubbard and Seiersen 2016, p. 12).

Despite that information security has become a hot topic in the boardroom, there is still a propensity for organisations to consider it as a challenge that the IT department must solve (Brotby 2009, pp. 1-3). When information security becomes siloed as a technical issue for the IT department, this negatively impacts the effectiveness of the information security (Brotby 2009, pp. 1-3) (Vroom and Von Solms 2004) (Herath and Rao 2009) (Ifinedo 2012). The purpose of Information Security Governance (IGS) is, therefore, to elevate information security into organisational governance, to ensure that it is represented and embedded across organisational strategies, structures and processes (Johnston and Hale 2009) (von Solms 2006) (Brotby 2009, pp. 1-8). ISG is commonly represented by defined strategies, policies, procedures, structures and processes defined by the top management (Brotby 2009, pp. 1-8) (Warkentin and Johnston 2008) (von Solms 2006) (Whitman and Mattord 2011, p. 24). ISG seeks to ensure that there is an alignment between organisational objectives and information security.

2.2.3 Information Security Integration and Organisational Alignment

There is a wide variety of organisations, but at its core an organisation can be considered a collection of capabilities organised to achieve a certain purpose (Jackson and Rahman 2017, p. 44). For this thesis, organisational capabilities will be defined as activities and processes, and the understanding of how these should be integrated and deployed to achieve the organisational objectives (Hall, Sarkani and Mazzuchi 2011, p. 156) (Hall, Sarkani and Mazzuchi 2011, p. 156) (Van Der Merwe 2002, pp. 407-408) (Chang, Chen, and Chen 2011, p. 150). The discourses informed by the literature on organisational capabilities have asserted that technical security controls are not sufficient to achieve information security resilience (Soomro, Shah and Ahmed 2016) (Hall, Sarkani and Mazzuchi 2011) (Farahmand, Atallah and Spafford 2012). For adequate efficiency, it is recognised that information security must be manifest in the activities, processes and objectives across the entire organisation (Whitman and Mattord 2011, p. 24) (Kayworth and Whitten 2010) (Jackson and Rahman 2017) (Hall, Sarkani and Mazzuchi 2011) (Vroom and Von Solms 2004) (Herath and Rao 2009) (Ifinedo 2012) (Da Veiga and Martins 2015). This will translate into a condition where the organisational objectives and the information security endeavours coincide and consolidate, achieving what is defined as strategic or organisational alignment (Chang, Chen, and Chen 2011, p. 152) (Brotby 2009, pp. 11-12). Research has shown that there is a positive correlation between the alignment with organisational objectives and the effectiveness of the information security (Chang, Chen, and Chen 2011, pp. 159-160) (Brotby 2009, pp. 11-12).

Despite this correlation, information security is often a result of responsive actions (Johnston and Hale 2009). This has resulted in the information security measures becoming dilatory additions (Johnston and Hale 2009) (Whitman and Mattord 2011, pp. 34-36). When the information security is a mere additional element outside the organisational objectives and strategies, it does not achieve the necessary alignment (Johnston and Hale 2009) (Whitman and Mattord 2011, pp. 34-36). The reasons as for why information security is not represented in the organisational objectives can be many (Anderson 2010). However, there are two reasons which are of particular relevancy for this thesis:

1) Because the information security is not properly represented in the organisational governance; and/or
2) Because the information security is not being promoted and enacted by the management (Straub and Welke 1998) (Farahmand, Atallah and Spafford 2012) (Whitman and Mattord 2011, p. 24) (Kayworth and Whitten 2010) (Soomro, Shah and Ahmed 2016)

(Jackson and Rahman 2017) (Hu, Dinev, Hart, and Cooke 2012) (Whitman and Mattord 2011, pp. 34-36).

For the purpose of this thesis, the concept 'information security alignment' will be used to refer to a state where the information security of an organisation has been integrated across the organisation as intended by the ISMS. Hence, when referring to information security integration, this describes a part of the alignment process.

2.2.4 Information Security Culture and Management Role

Organisational culture and the development of said culture is an extensive topic which would be outside of the scope of this thesis to dive into (Schein 2010). The coverage of the topic will therefore remain superficial, yet sufficient to root the thesis in the field. It is argued that all organisations contain a dominant culture, often representing the overarching organisational objectives, and subcultures, representing organisational units or third parties (Da Veiga and Martins 2017) (Schein 2010, pp. 55-72). The organisational culture encompasses elements, such as norms and assumptions, related to the objectives which an organisation is seeking to achieve (Schein 2010 pp. 35-54).

Information security culture refers to two aspects: the first aspect refers to the objectives of an organisation's information security, which comes down to confidentiality, integrity and availability (Martins and Elofe 2002) (Stamp 2011, p. 2). The second refers to the elements which make up the assumptions, norms and behaviours which are acceptable and necessary to enact the information security (Da Veiga and Martins 2017) (AlHogail and Mirza 2014) (Martins and Elofe 2002). In other words, information security culture largely refers to what is known as 'the human factor' of security (Van Niekerk and Von Solms 2006) (Da Veiga and Martins 2015) (AlHogail and Mirza 2014).While there is an aspiration for information security culture to be a part of the dominant culture, there is a clear tendency for it to rather manifest itself in various subcultures (Da Veiga and Martins 2017). These subcultures can either align themselves with the dominant culture, or oppose it, in which case incongruences can appear (Da Veiga and Martins 2017). It is argued that these subcultures need to be identified and understood, as a part of the desire to integrate information security into the organisational activities and processes (Da Veiga and Martins 2017) (AlHogail 2015) (Martins and Elofe 2002). To achieve this, management is identified as a decisive actor (Knapp, Marshall, Rainer and Ford 2006) (Van Niekerk and Von Solms 2010) (Martins and Elofe 2002).

For the purpose of this thesis, the definition of management has unambiguously been borrowed from literature on the strategic alignment of information security. According to this definition, one of the determining responsibilities of management is to '*articulate, motivate and direct the fulfilment of strategic goals and objectives*' (Anderson 2010, p. 3). Because risk management has become an integral part of organisations' strategic goals and objectives, management is supposed to provide such guidance within information security as well (Anderson 2010, p. 3) (Straub and Welke 1998) (Farahmand, Atallah and Spafford 2012) (Whitman and Mattord 2011, p. 24). In other words, management can be considered one of the most important roles in the effort to link organisational activities, processes and objectives with the information security. This will, however, depend on how the information security is understood by the management (Warkentin and Johnston 2008, pp. 47-48) (Farahmand, Atallah and Spafford 2012, p. 243) (Straub and Welke 1998, pp. 441-442). Research has suggested that management perception and understanding of information security is shaped by three dimensions in particular:

1. The organisational perspective on information security as a risk;
2. by the types and scope of the information security measures introduced into their systems;
3. and by their own individual knowledge and understanding of information security (Straub and Welke 1998) (Goodhue and Straub 1991).

In other words, while management is identified as a decisive actor in implementing an information security culture, their ability and/or incentive to do so will depend on both individual and organisational factors.

2.2.5 Information Security Management System (ISMS)

Reducing risk and protecting organisational values remain a pressing issue for most organisations. One of the most common means to systematically address this is through the adoption of an Information Security Management Systems (ISMS) (Disterer 2013) (Humphreys 2008) (Fenz, Heurix, Neubauer and Pechstein 2014). While there is a variety of ISMSs, there are two which are of particular relevancy for this thesis. These are ISO/IEC 27001 and NIST CSF (drawing upon NIST SP 800-53) (ISO/IEC 2013) (NIST CSF 2018) (NIST 2013). While there are differences between them, they also share a lot of commonalities. These standards provide organisations with lists of controls for the purpose of managing the information security risk associated with their information systems (ISO/IEC 2013) (NIST CSF 2018) (NIST 2013). By controls it is meant safeguards or countermeasures which are designed to:

1. Protect the confidentiality, integrity and availability of the information which is processed, stored, transmitted or otherwise utilised by the organisation; and
2. Ensuring that an organisation meets the necessary security requirements (ISO/IEC 2013) (NIST CSF 2018) (NIST 2013).

The standards seek to provide organisations with guidance on the implementation of controls, which include guidelines on policies, procedures, organisational structure, and software and hardware functions (ISO/IEC 2013) (NIST CSF 2018) (NIST 2013). The purpose is to guide organisations to meet their security needs, and thereby enable the organisation to reach their organisational objectives (ISO/IEC 2013) (NIST CSF 2018) (NIST 2013). It must be stressed that ISMS are holistic and do not merely provide guidance for those who work with IT. ISO specifies that '*the security that can be achieved through technical means is limited and should be supported by appropriate management and procedures*' (ISO/IEC 2013, p. vi). Moreover, it specifies that the identification of the correct controls will demand careful planning, and an effective ISMS requires the support of all employees (ISO/IEC 2013, p. vi).

The purpose of an ISMS is multifaceted, but among the objectives is to align an organisation's information security better with its organisational objectives and risk management (Brotby 2009, pp. 64-65) (Whitman and Mattord 2011, pp. 195-204). By doing so they seek to embed an understanding of information security as an organisational-wide concern (Brotby 2009, pp. 64-68) (Whitman and Mattord 2011, pp. 195-204). Moreover, they seek to coax organisations to appreciate that managing these risks require strategic and coordinated efforts by organisational management and leadership (Brotby 2009, pp. 64-68) (Whitman and Mattord 2011, pp. 195-204). Throughout this thesis, ISMS and information security will be used somewhat interchangeably. However, for the purpose of this thesis, ISMS will refer to the formalised system and approach an organisation has regarding information security. While information security will refer to the enactment of an ISMS (or merely the adherence to information security principles, in cases where there is no ISMS).

2.3 Structuration Theory

Structuration theory, as articulated by Anthony Giddens, has served two purposes for this inquiry. Firstly, it has provided the epistemological lens which has formed the bedrock of how the studied problem has been understood. Secondly, it has served as the theoretical framework through which the problem has been analysed. It must be noted that Giddens has been a prolific academic and writer, leading his contributions to being both expansive and complex (Jones, Orlikowski and Munir 2004, pp. 298-300). It is therefore far outside the scope of this thesis to truly explore the extents and intricacies of his work. Due to this, primary literature was principally utilised to outline the foundational principles of structuration theory. Secondary literature has been used to contextualise and make sense of the theory in reference to the fields of Information Systems and Information Security. This has been done with the awareness that it can be a possible pitfall to utilise a too narrow sliver of Giddens's primary work (Jones, Orlikowski and Munir 2004, pp. 298-300). It has also been done acknowledging the criticism that the theory is sometimes utilised in a notably detached way from its original context (Walsham and Han 1991, pp. 56-58). Yet, Giddens himself has stated that he prefers researchers to import concepts in a 'sparing' and 'critical fashion', rather than to adopt the whole framework from one study to another (Jones and Karsten 2008, p. 134). Hence, for this study, structuration theory has been used both as a novel, practical problem-solving methodology, and as an academic tool for theory-development.

In its original form, structuration theory sought to end a century old debate, or the binary 'empire-building' as put by Giddens, about the ontological nature of social reality (Giddens 1984, pp. 1-3) (Jones, Orlikowski and Munir 2004, pp. 300-301). One school of thought, the objectivists, considered that structure inevitably imposes restrictions on agency (Giddens 1984, pp. 1-3). This would indicate that structure guides agency, leading to the agent being of limited importance in understanding a social system (Giddens 1984, pp. 1-3). The opposing school of thought, the subjectivist, viewed it the other way around. According to this perspective, structure was largely a result of agency; it was human will and action that shaped a social system into what it was (Giddens 1984, pp. 1-3). With structuration theory, Giddens sought to end this dichotomy between structure and agency (Giddens 1984, pp. 1-5) (Giddens 1979) (Orlikowski and Robey 1991) (Jones, Orlikowski and Munir 2004). Consequently, structuration theory can be considered a tool to overcome this discord.

Giddens built his theory on a distinct definition of structure. Social, human action can be considered recursive (Giddens 1984). In other words, the social actor does not forge actions out of a vacuum; they recreate them from antecedent conditions (Giddens 1984, pp. 1-26). In the process of recreating these actions, the social actor simultaneously recreates the conditions which make these actions possible (Giddens 1984, pp. 1-26). Giddens thus refers to structure as '… *structuring properties allowing the "binding" of time-space in social systems* …' (Giddens 1984, p. 17), explaining that this is what allows the seemingly systematic recursiveness of social practices across time and space (Giddens 1984). This takes form as 'structural properties' exhibited by social systems (Giddens 1984, pp. 17-27). This process is what becomes referred to as the *duality of structure* (Giddens 1984, pp. 23-27). This indicates that structure exists only through the day-to-day activities of social agents and does not exist in and of itself (Giddens 1984, p. 26). It is, thus, important to note that although the structure conditions the actor to recreate the structure, it is not the structure that autonomously recreates itself.

Giddens developed an interconnected framework of concepts to explain how structure manifests itself into actions, and vice versa. Due to the limitations of space and scope in this paper, these concepts will be simplified and tailored to the objective of this study. Nevertheless, a general overview of the framework will be provided. Critical to the production and reproduction of structures in social systems are the three dimensions of structure referred to as *signification, domination* and *legitimation*, as can be seen in Figure 2.1 (Giddens 1984, pp. 28-29) (Giddens 1979, pp. 81-82). When viewed in the interaction between people and structure these dimensions are referred to as *modalities of structuration* (Giddens 1984, pp. 28-29) (Giddens 1979, p. 81).

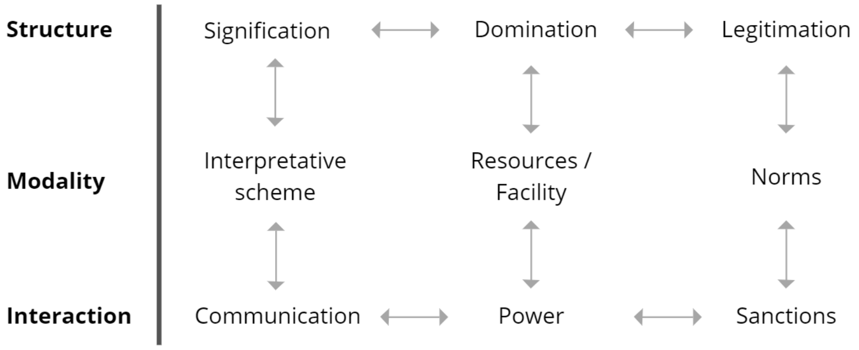


Figure 2.1 – Modalities of Structuration

(Giddens 1984, p. 29)

The modality for signification is referred to as *interpretative schemes*, which Giddens explains that '*... form the core of mutual knowledge whereby an accountable universe of meaning is sustained through and in processes of interaction*' (Giddens 1979, p. 83). In other words, interpretative schemes are the shared knowledge people utilise in the shaping and sustaining of social interaction (Jones and Karsten 2008) (Orlikowski and Robey 1991). The modality for domination is referred to as *resources* (or *facility*) and is defined as the 'transformative capacities' which enables command over objects and people, to exercise power and to achieve goals (Giddens 1984, p. 33) (Giddens 1979, pp. 91-93) (Orlikowski and Robey 1991). The modality for legitimation is *norms*, which are described as the organisational rules which, through sanctions, govern legitimate, appropriate and inappropriate conduct (Orlikowski and Robey 1991) (Giddens 1979, pp. 97-98) (Giddens 1984, pp. 29-33). These modalities are drawn upon by the agent as they produce and reproduce the structure, while the modalities themselves are affected by the same dynamic (Giddens 1979, p. 81) (Orlikowski and Robey 1991). Put in more tangible terms, the modalities of structuration can be considered the sources which shape the activities and process which are considered logical and purposeful in an organisation. It can also be compared to the concept of a reinforcing feedback loop which servers to perpetuate a system, as utilised within systems thinking (Meadows 2008, pp. 11-74). These concepts are complex and comprehensive, and engaging with them on an abstract theoretical level is not within the scope of this thesis. However, these modalities offer a clear, practical possibility of identifying and analysing existing social systems within an organisation and have therefore served as the conceptual framework underpinning the research conducted in this thesis.

2.3.1 Structuration Theory in Information Systems

Structuration theory is a social theory hailing from sociology and has thus been imported into the field of Information Systems. Additionally, Giddens does not dedicate significant attention to the role of information systems in relation to his own work on structuration theory (Poole and DeSanctis 2004, pp. 208-211) (Orlikowski 2000, p. 405). Despite this, it has been recognised that structuration theory has provided Information Systems research with new and vital capacities to analyse and understand the interaction between people, actions and information technology (Poole and DeSanctis 2004) (Orlikowski and Robey 1991). For the purpose of this paper, there are particularly two aspects which will be identified as of particular relevance. The first aspect is possibly the most obvious one: the structures within an organisation. When we speak of an organisation, we do not refer to the buildings it is located in or similar forms of physical assets; we refer to the people, the activities and the purposes within the organisation (Jones, Orlikowski and Munir 2004, pp. 302-303) (Tolbert and Hall, pp. 34-36). An organisation operates with a specific purpose, identified through its organisational objectives. When people join such an organisation, they will join existing structures which postulate certain types of activities and processes as purposeful (Jones, Orlikowski and Munir 2004, pp. 302-303). The employees will then be conditioned, both knowingly and unknowingly, into the practices of the organisation. Yet, those activities and processes are not permanently ingrained into the organisation; they are sustained by the day-to-day actions of the people in it (Jones, Orlikowski and Munir 2004, pp. 302-303). Implicitly, if the daily activities change, then the structural properties will change (Jones, Orlikowski and Munir 2004, pp. 302-303). Structuration theory, thus, offer a unique insight into the potential rigidity and/or malleability of organisations, and the role of structure when new information systems are introduced.

The second aspect is how structuration theory can help elucidate what effect new information systems can expect to have on the organisation it is introduced into. Orlikowski and Robey (1991) expound that the same inherent duality presented by Giddens can be found within information systems. This is because the enactment of information systems in an organisation can be considered a structure (Orlikowski 2000, pp. 409-410). Information systems has both a constituted nature and a constitutive role: meaning that it is a product of social action in a specific structural context, while simultaneously serving as a mediator and constrainer of social action (Orlikowski and Robey 1991). Information systems can thus be considered a genesis of organisational action, while also being a culmination of organisational activities (Orlikowski and Robey 1991). In other words, the recursive and reciprocal influence flowing between agent and structure, the reinforcing feedback loop, is also present between information systems and the organisation. The organisation shapes the information systems, while the information systems simultaneously shapes the organisation, as illustrated by Figure 2.2.

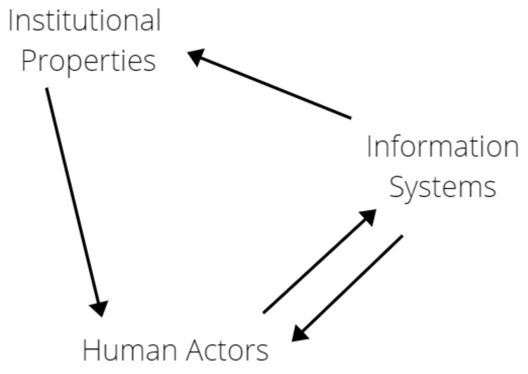


Figure 2.2 – Feedback loop

(Derived from Orlikowski and Robey 1991)

When information systems seek to overturn or change the existing structures, it will often go against the established structures of an organisation, and the actors might potentially respond with subversion or resistance (Orlikowski and Robey 1991). If the actors respond to a new information system by not employing it, the system will not get an opportunity to initiate the process of structuration. Without this process, where the system is embedded into the daily activities of the organisation, the system will be rendered impotent in its objective to shape organisational action (Orlikowski and Robey 1991). Structuration theory, thus, serves to explicate how information systems, or information security in this case, can be considered a tool of structuration within organisations. Identifying and understanding the structures of an organisation will, thus, enable you to identify the recursive feedback loops.

3. Methodology

AR and ADR have a twofold imperative: solving an organisational problem, and engaging in scientific research (McKay and Marshall, p. 141). Because of this, McKay and Marshall have put forward a proposition for two different types of methodologies in an AR or ADR projects (McKay and Marshall, pp. 141-148). The research methodology (M_R) and the problem-solving methodology (M_{PS}).

1) The research methodology (M_R) is the methodology which has been utilised for the academic research. This has provided the overarching strategy and guidance on the research process, data collection, and the general thesis formulation.
2) The problem-solving methodology (M_{PS}) is the methodology which has sought to solve the organisational problem. An existing theoretical framework created by Orlikowski (2000) was repurposed to create the problem-solving methodology.

From the outset, it was clear that a form of Action Research (AR) was the necessary research methodology for the study. This is because the author participated in the organisational context as an employee. However, due to limitations on time, it would not be possible to engage in the necessary iterative cycles for the purpose of implementing change, which tend to be necessary for proper Action Research. Due to this, Action Research Design (ADR), as proposed by Sein, Henfridsson, Purao, Rossi, and Lindgren, was decided upon as a more adequate methodology (Sein et al. 2011). ADR aligns more with the scope of the thesis, because of its focus producing formalised learning regarding an IT artefact. ADR has therefore constituted the dominant methodological approach, with supplementations from AR. The methodology has been adhered to as closely as possible, but exceptions have been made where the thesis has not been able to engage in the necessary iteration or building of the artefact. ADR serves as the principal methodology, but because AR has provided supplementary guidance, both methodologies are covered in this chapter.

Due to the complex amalgamation of various methodologies and theoretical frameworks, the methodology chapter has become somewhat voluminous. There are two reasons for this:

1) The first was inevitably to ensure the academic rigidity of the thesis. Due to the situational nature of the study, considerable efforts have been made to ensure its recoverability.
2) The second reason is because it has not been possible to fully observe all the ADR steps. More specifically, the steps concerned with building, intervention and evaluation (BIE) of an IT artefact have not been possible to execute. This is due to the limited time that prevented the project from engaging in the BIE cycles of the ISMS (the IT artefact). Instead, the focus has been put on the formalised learning. A notable part of the chapter has therefore been dedicated to explaining this.

The methodology chapter can be separated into two different parts. Sections 3.1 to 3.4 is a literature review of the AR, ADR and Orlikowski's theoretical framework. Here the concepts and steps within the methodology will be clearly explained. In section 3.5 and 3.6, the methodological concepts and steps of the first section will be adapted and fitted to be employed for the research project of this thesis.

3.1 Action Research

Action Research (AR) emerged from the reflection that studying change in social conditions could not adequately be done in laboratorial conditions. Such a sterile setting would make an artificial representation of social reality, which would fail to account for the constant flux of social conditions (Checkland and Holwell 2007). At its essence, AR is therefore based on the recognition that social conditions are predisposed to change, rather than consistency (Checkland and Holwell 2007). Due to this predisposition, AR is utilised under the assumption that complex social conditions can best be understood by attempting to introduce change into the social condition (Baskerville 1999). A defining aspect of AR that separates it from other qualitative approaches is, thus, that the researcher is actively involved in planning change as a part of the research (Avison, Baskerville and Myers 2007). AR offers the researcher a multitude of valuable benefits. Among them it is specifically worth to note how AR bridges the academic field of Information Systems (IS) to the empirical reality of information systems in organisational life. As a methodology, AR offers the potential for both contributing to IS as an academic field, while also solving concrete and relevant problems in organisations (Lee 2007) (Baskerville 1999). This duality enables this thesis to both address an organisational problem and contribute towards filling an academic knowledge gap.

Criticism has been leveraged at AR, however, due to its interpretative, conditional and somewhat subjective nature (Checkland and Holwell 2007). Typically, scientific research is considered methodologically proper by reductionism, repeatability and refutation (Checkland and Holwell 2007, p. 5). Because AR is concerned with social change, recreating the conditions necessary to scientifically repeat AR research is difficult and infeasible (Checkland and Holwell 2007). As an alternative, it has suggested that it should at least be possible for the research to be *recoverable* (Checkland and Poulter 2010, p. 196). By recoverable it is meant that other researchers will be able to discern and pinpoint what was done to achieve the results that were acquired and the conclusions which were made (Checkland and Poulter 2010, p. 196). Consequently, it is proposed that a more rigorous structure, containing a clear epistemological approach and declared-in-advance methodology, is used (Oates 2005, pp. 156-157) (Checkland and Holwell 2007). Peter Checkland's conceptualisation of F, M and A is considered to lend AR with this structure, and is thus viewed by this thesis as an effective way to universalise the research done in this thesis (Oates 2005, pp. 156-157) (West and Stansfield 2001, pp. 254-256).

3.2 Peter Checkland's F M A

The F M A seeks to provide AR with a clear epistemology that provides the research scientific rigour and ensures its recoverability (West and Stansfield 2001). It contains the following three concepts:

Table 3.1 – Checkland's FMA

Concept	**Description**
F: Framework of Ideas	The Framework of Ideas act as a theory which provides epistemological guidance to the research (Checkland 1995) (Checkland and Holwell 2007) (McKay and Marshall 2007, pp. 144-147) (West and Stansfield 2001) (Oates 2005, pp. 156-157). This

	guidance provides conceptual rigour which allows the researcher to make sense of the research according to discernible reference points, while also providing clarity to other researchers about the epistemological assessments which have been made (Checkland 1995) (West and Stansfield 2001) (Oates 2005, pp. 156-157).
M: Methodology	The Methodology arguably refers to two distinct aspects: the problem-solving methodology, and the research methodology (McKay and Marshall 2007). Research methodology (M_{R}) is the overarching research design of the thesis, while the problem-solving methodology (M_{PS}) is the implementation of F into a methodology to address A (McKay and Marshall 2007).
A: Area of Application	The Area of Application is the real-world problem situation which initiated the research, and which is being addressed by the research (Oates 2005, pp. 156-157). The A will offer the researcher learning about the problem situation, as well as learning about how the F and M contribute towards solving the A (West and Stansfield 2001, pp. 254-256) (Oates 2005, pp. 156-157).

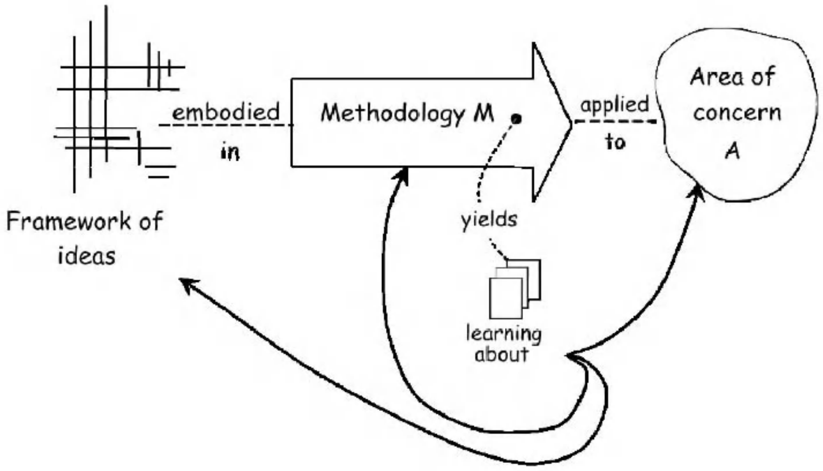


Figure 3.1 – Checkland's FMA

(Checkland and Holwell 2007, p. 8)

The F M A must be declared in advance, to provide AR with scientific rigour and conceptual clarity (Checkland and Holwell 2007, pp. 7-9). Yet, it is equally important to acknowledge that the F M A should not be unbending. The F M A is a process which will require reflection on the experience that has been made (Checkland and Holwell 2007, pp. 9-10). The researcher must, thus, assess the adequacy of the F M for understanding and enacting action for A, and determine whether F M need to be changed (Checkland and Holwell 2007, pp. 9-10) (West and Stansfield 2001, pp. 274-275). Figure 2 demonstrates the potential cyclical nature of the F M A.

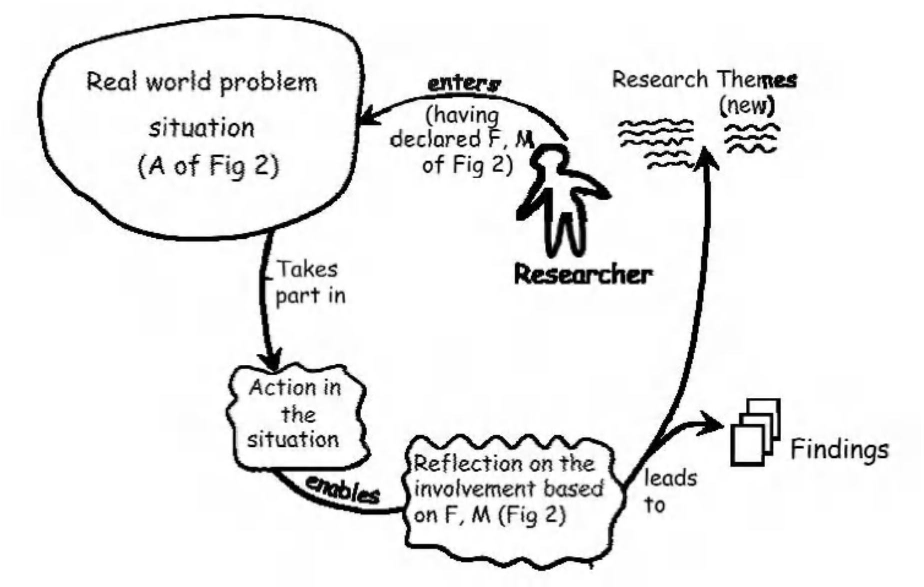

Real world problem situation (A of Fig 2)
enters
(having declared F, M of Fig 2)
Research Themes
(new)
Researcher
Takes part in
Action in the situation
enables
Reflection on the involvement based on F, M (Fig 2)
leads to
Findings

Figure 3.2 – F M A Cycle

(Checkland and Holwell 2007, p. 9)

3.3 Action Design Research (ADR)

In simplified terms, Design Research (DR) is concerned with the development of design knowledge through the building and utilisation of IT artefacts (Sein et al. 2011, p. 39) (Hevner 2007). DR is a vast field with a number of affiliated methodologies (Sein et al. 2011) (Hevner 2007) (Hevner and Chatterjee 2010). Consequently, it is not within the scope of this thesis to cover them all. Focus has therefore been put on the literature discussing the most relevant versions, which is mostly represented by the paper provided by Sein, Henfridsson, Purao, Rossi and Lindgren (2011). According to this perspective, DR is concerned with ensemble artefacts. By ensemble artefacts it is meant how the organisational structure shapes the use of an organisation's hardware and software (Sein et al. 2011, p. 38). This indicates the technical parts and the organisational context of an organisation cannot be separated but must be perceived as forming an interactive whole which shapes each other (Sein et al. 2011, pp. 38-39). This means that the ensemble artefact emerges not merely from design, but through a balance between design and use (Sein et al. 2011, p. 39). This will be considered to be largely aligned to how structuration theory views the correlative process of structuration to happen between structure and activity. For this thesis, the ISMS at NorAg will be considered the IT artefact.

Design Research and Action Research share numerous traits that make their merger seem purposeful and beneficial (Sein et al. 2011) (Lee 2007) (Baskerville and Wood-Harper 1998). This includes, but is not limited to, a focus on solving real world problems; organisational participation and intervention; and a recognition that there is a level of organisational emergence that cannot be controlled by researchers (or designers) (Sein et al. 2011, pp. 37-39) (Lee 2007). These overlapping similarities have instigated a number of attempts to combine Action Research with Design Research (or contrariwise) (Sein et al. 2011, p. 39) (Lee 2007, pp. 49-50) (de Figueiredo, Dias and da Cunha 2007). This is what we will refer to as Action Design Research (ADR), according to the definition provided by Sein et al. (2011).

There are in particular two aspects of ADR that makes it particularly apt for this thesis. The first is the recognition of the pivotal link between IT artefacts and the organisation. ADR recognises that organisational use of an IT artefact will shape its design and can lead to unintended and unanticipated consequences (Sein et al. 2011, pp. 39-40). This recognition compliments the analysis done in the thesis. Secondly, a central part of AR is the ability to engage in research cycles. Due to the time limitations of this thesis, as a part of a postgraduate degree, such long-term commitment has not been possible. The ADR proposed by Sein et al. has cycles as a potentially integrated part of the methodological framework, but their role is not as definitive as in AR (Sein et al. 2011, p. 38) (Hevner 2007). Instead, their ambition is for ADR to incorporate the cycles proposed by Hevner (Hevner 2007), while also being a concerted research effort with a clearer start and end, as displayed in Figure 3.3 (Sein et al. 2011, p. 38). The possibility of ending without cycles is also supported by the literature on Soft Systems Methodology (SSM), where Checkland and Poulter assert that some studies can end after having defined the necessary actions, rather than after implementing the action (Checkland and Poulter 2010, p. 207). Because it will not be possible to engage in the cycles, the focus of this thesis has been on the formalised learning.

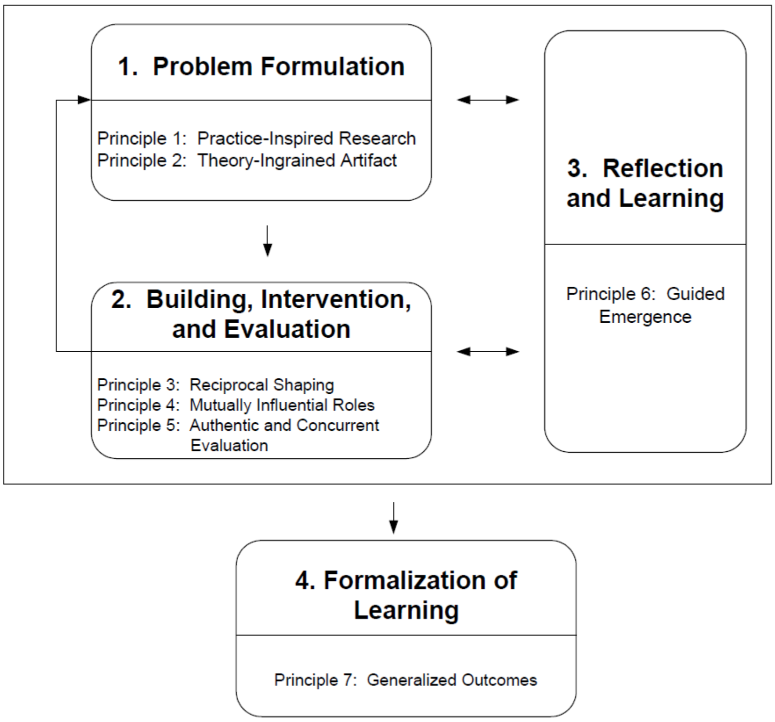

1. Problem Formulation
Principle 1: Practice-Inspired Research
Principle 2: Theory-Ingrained Artifact
2. Building, Intervention, and Evaluation
Principle 3: Reciprocal Shaping
Principle 4: Mutually Influential Roles
Principle 5: Authentic and Concurrent Evaluation
3. Reflection and Learning
Principle 6: Guided Emergence
4. Formalization of Learning
Principle 7: Generalized Outcomes

Figure 3.3 – Action Design Research

(Sein et al. 2011, p. 41)

3.3.1 The ADR Stages

The ADR in question is divided into four stages which contain in total six principles. Although they will be explained as separate categories with affixed definitions, it is important to bear in mind that they are often overlapping and/or concurrent. These are, as defined by Sein et al (2011):

Table 3.2 – Action Design Research Stages

Stages / Principles	**Description**
Stage 1: Problem Formulation	The problem formulation is concerned with identifying the problem, articulating the research question, and exploring the purview of the research (Sein et al. 2011, p. 40). This stage also involves the conceptualisation of the research based on existing theories and technologies (Sein et al. 2011, p. 40).
Principle 1: Practice-	ADR research ought to emerge out of a problem, but these problems ought to be considered as opportunities for knowledge

Inspired Research	production, not merely a contextual situation to be solved (Sein et al. 2011, p. 40).
Principle 2: Theory-Ingrained Artefact	The ensemble artefact should be constructed and evaluated with relevant theories, thus making the theories socially manifest (Sein et al. 2011, pp. 40-41).
Stage 2: Building, Intervention, and Evaluation (BIE)	In stage two, the framed problem and theoretical framework create the premises for which the initial design can be made (Sein et al. 2011, p. 41). This stage also contains the iterative cycle between *building* the artefact, *intervening* into the organisation with the design, and *evaluating* its ability to lead to the desired effects (Sein et al. 2011, pp. 41-42). The evaluation is concerned with assessing how the original build functions in the organisational setting which it is implemented. The evaluation is therefore continuous, rather than something which is done at the end (Sein et al. 2011, pp. 41-42).
Principle 3: Reciprocal Shaping	This principle stresses the parallel pressure emitting between the IT artefact and the organisational context (Sein et al. 2011, pp. 42-43).
Principle 4: Mutually Influential Roles	This stresses the mutual learning that ought to occur in ADR projects where there is an amalgamation of researchers and practitioners with various forms of expertise and perspectives (Sein et al. 2011, p. 43).
Principle 5: Authentic and Concurrent Evaluation	ADR omits a stage-gate approach and has evaluation as an integrated and continuous part of the process, meaning that it happens throughout, and not merely at the end, of a project (Sein et al. 2011, pp. 43-44).
Stage 3: Reflection and Learning	The stage for reflection and learning have two distinct aspects to it. The first is the continuous reflection on how the different parts of the research affects each other. The manner in which the

	problem was framed; the employed theories; and the emerging ensemble, must all be evaluated and refined as artefact and the research evolves (Sein et al. 2011, p. 44). The second is how to transform contextual learning to general knowledge. This is based on the foundational notion that, in academia, solving a problem is not sufficient on its own; one ought to extract knowledge that can be conceptualised or generalised for application elsewhere (Sein et al. 2011, p. 44). Hence, the researchers must be receptive to and active at identifying discernible patterns and principles (Sein et al. 2011, p. 44).
Principle 6: Guided Emergence	At its core, ADR acknowledges that the preliminary design must be considered emergent, as the design will be moulded by organisational use, perspectives and participants (Sein et al. 2011, p. 44).
Stage 4: Formalisation of Learning	The last stage is a fluid continuation of stage three. Here the situated learning will be elevated into conceptual discoveries which can serve to provide principles, theory adaptions, and other insight which can be employed in future research (Sein et al. 2011, p. 44). This will be possible by reconceptualising the problem, the solution and the learning into classes (of problems, solutions and learning), rather than leaving them as situated, stand-alone elements (Sein et al. 2011, pp. 44-45). Irrespectively of whether the ensemble design was successful or not, the formalised learning will become a pivotal product of the research (Sein et al. 2011).
Principle 7: Generalized Outcomes	While the ensemble which is being studied is highly situational, ADR seeks to elevate the experiences made into generic principles (Sein et al. 2011, pp. 44-45). This is largely done by '(1) generalization of the problem instance, (2) generalization of the solution instance, and (3) derivation of design principles from the design research outcomes.' (Sein et al. 2011, p. 44).

3.4 The Problem-solving Methodology (M_{PS})

Giddens maintained that '*the modalities of structuration are drawn upon by actors in the production of interaction*' while simultaneously being the '*media of the reproduction of the structural components of systems of interaction*' (Giddens 1979, p. 81). It is recognised that all human interaction intrinsically contains these modalities, which fuses the sphere of social action with that of structure (Orlikowski and Robey 1991, p. 148). Due to this, Giddens has considered that all interaction between action and structure can be analysed in terms of these modalities (Orlikowski and Robey 1991, p. 148). This thesis has therefore utilised a repurposed version of the lens developed by Orlikowski (2000) to analyse the information security at the NorAg. This is further elaborated on in section 3.5.3.

Table 3.3 – M_{PS} – Problem-solving Methodology

Modality	**Resources**	**Norms**	**Interpretative schemes**
Description	Resources refer to a transformative capacity to command objects or other material phenomena, as well as people (Jones and Karsten 2008, p. 130). This enables the realisation and accomplishment of intentions and goals, and the exercise of power (Orlikowski and Robey 1991, p. 148). This could, for example, take the form of the decision-making power wielded by an employee	What is correct or incorrect behaviour and practices are embedded in a sanctioned, moral setting (Orlikowski and Robey 1991, p. 148). This means that when a person chooses how to act, they assess what behaviour is aligned with the dominating norms and standards of the applicable social setting (Walsham and Han 1990, p. 54). In practice, these norms could take the form of a user guidance or an	The stocks of knowledge which humans draw on to make sense of behaviour and circumstances (Orlikowski and Robey 1991, p. 148) (Whittington 2015, p. 148) (Walsham and Han 1990, p. 54). This takes the form of knowledge, assumptions and expectations acquired through previous communication, training and

	(Whittington 2015, p. 148), but when applying it to Information Systems Orlikowski refers to it as the IT systems/technology available to employees (Orlikowski 2000).	organisational policy, describing correct use of a technology (Orlikowski 2000, pp. 412-413).	experiences (Orlikowski 2000, pp. 409-410).

3.4.1 Orlikowski's Lens for Enactment of Structures in Practice

Systems can be considered to be a form of structure (Orlikowski 2000). This implies that there is same type of recursive reciprocity between technology and social action, as there is between structure and social action (Orlikowski 2000). This is exemplified in Figures 3.4 and 3.5. When people utilise information systems, there are two distinct aspects at work. The technology has been inscribed with properties and functionalities which enables and delimits what the user can do with it (Orlikowski 2000, pp. 409-411). Thereby, the information systems are imposing a certain structure upon the user. Simultaneously, the user bases their usage on the skills, power, knowledge, expectations and assumptions which they have acquired previously through informal and formal experiences (Orlikowski 2000, pp. 409-411). The user is, hence, exerting an influence over how the information systems is used, rooted in the previous structures which the user has been exposed to. This signifies that the structures of information systems will always be situated within a complex nexus of other social structures (Orlikowski 2000, p. 411). While some structures can be expected to exert more influence than others, the distribution of influence is not fixed. Through the exposure to new knowledge, understanding and motivations, people might become more open to some structure; less open to others; and/or start exerting more influence on a structure than the structure exerts on the person (Orlikowski 2000, pp. 411-412). The introduction of a new organisational policy describing the correct use of a technology might, for example, change the existing use of that technology to comply better with the new policy (Orlikowski 2000, p. 412). In such a case, a new structure might replace an old one.

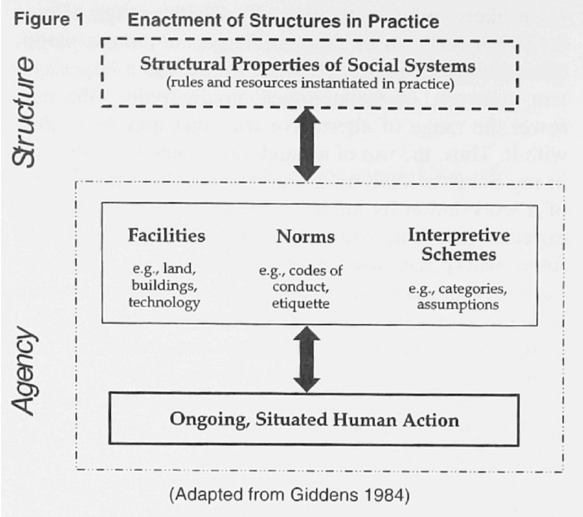


Figure 1
Enactment of Structures in Practice
Structure
Structural Properties of Social Systems
(rules and resources instantiated in practice)
Facilities
e.g., land, buildings, technology
Norms
e.g., codes of conduct, etiquette
Interpretive Schemes
e.g., categories, assumptions
Agency
Ongoing, Situated Human Action
(Adapted from Giddens 1984)

Figure 3.4 – Enactment of Structure in Practice

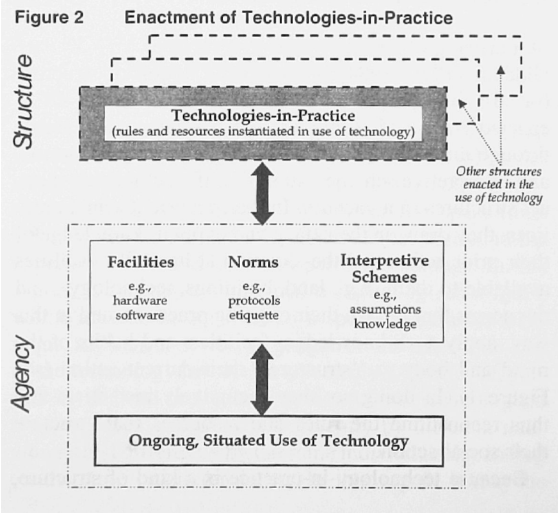


Figure 2
Enactment of Technologies-in-Practice
Structure
Technologies-in-Practice
(rules and resources instantiated in use of technology)
Other structures enacted in the use of technology
Facilities
e.g., hardware software
Norms
e.g., protocols etiquette
Interpretive Schemes
e.g., assumptions knowledge
Agency
Ongoing, Situated Use of Technology

Figure 3.5 - Enactment of Technologies-in-Practice

(Orlikowski 2000, p. 410).

In Orlikowski's study (2000), she applies this lens to three different organisations which have all implemented a new technological artefact called *Notes*. The properties of the technology largely revolve around collaboration and information sharing (Orlikowski 2000, p. 414). The study demonstrated a noticeable correlation between distinguishable structural properties reflected by organisational practices and processes, and the manner in which the technology was utilised (Orlikowski 2000). It was identified that organisations which were already accustomed to cooperation and teamwork were more prone to implement and utilise the technology and consider it beneficial (Orlikowski 2000). There were even differences within organisations, where one team with a collaborative mindset and experience found the technology useful, while another team with a more individualistic mindset and experience minimised the use (Orlikowski 2000).

3.5 The F M A; the ADR (M_R); and the Problem-solving Methodology (M_{PS})

The former sections were dedicated to properly reviewing the various methodological approaches and concepts which have been at play in the research. The rest of the chapter will be dedicated to demonstrating how this has been put into use. Sections 3.5.1, 3.5.2 and 3.5.3 therefore explain how the abovementioned concepts, stages and models have been utilised for this study. The last parts of this chapter provide an overview of the data collection.

3.5.1 The F M A

Table 3.4 – The FMA

Concept	
F: Framework of Ideas	The research of this thesis has happened based according to an epistemological framework informed by structuration theory. Information security has therefore been considered as a structure which is both the mediator of social action, while simultaneously being a product of social action. This means that for the information security to be integrated into the organisation, it must be enacted through activities and processes.
M: Methodology	There are two methodologies at play in this thesis. The research methodology (M_R) and the problem-solving methodology (M_{PS}). The M_R is represented by a customised ADR which has guided the research conducted for this project. The data collection has happened through document reviews and interviews. The customised version of the ADR is shown in Table 3.5. The M_{PS} is represented by Orlikowski's repurposed, theoretical lens, and is shown in Figure 3.6.
A: Area of Application	The practical purpose of the project is to explore and analyse challenges and solutions to information security alignment across the organisation. The academic purpose is to identify and analyse processes of structuration and their effects on information security alignment.

In this thesis, a well-established theory has been employed for F. The downside of this is that a formalised and structured theory can curb the ability of the researcher to identify and understand that which does not fit into the theory (West and Stansfield 2001, p. 268). The upside, however, is that the acceptance of the theory provides an increased experience of recoverability and a clearer understanding of its epistemological logic (Oates 2005, p. 157) (West and Stansfield 2001, pp. 268-269).

3.5.2 The Research Methodology (M_R)

One of the steps embodied by ADR is the focus on building, intervention and evaluation (BIE) which allows the researcher to iteratively build and evaluate the IT artefact (Sein et al. 2011). Because of the time and resource limitations of the thesis, this iteration has not been possible. Instead, the effort has dedicated to evaluating the ISMS. This evaluation has been done through the application of the theoretical framework, which allowed for the identification and assembly of five different types of structure.

Table 3.5 – Research Methodology – ADR

Research Methodology (M_R) – Action Design Research	
Stages	**IT Artefact / Problem-Solving Methodology (M_{PS})**
Stage 1: Problem Formulation	
The outline of the organisational problem was first identified in coordination with the information security team at NorAg, with a researcher-client agreement. This provided the foundational guidance for the preliminary research, which was conducted on the organisation's available information security documents. Based on this, the problem formulation was articulated as: PF: What causes the organisational challenges with integrating the ISMS across the organisation, and how can the ISMS better align itself with organisational activities and processes. To provide a possible explanation and solution with theoretical soundness, structuration theory was employed. Structuration theory postulates that there is a	*Recognition of the IT artefact*: The official ISMS requires alignment across the organisation. Based on documents produced through security audits and assessments, the IT department did not consider this to be adequately achieved at the current moment. This was not achieved because the ISMS was largely siloed to the IT department, shifting the responsibility of information security from the organisation as a whole, to the IT department in specific. *The problem-solving methodology (M_{PS})*: To be able to analyse the problem, the M_{PS} was built, based on Orlikowski's theoretical lens. The purpose of the M_{PS} is to identify and understand structures at NorAg.

reciprocal relationship between institutionalised structures and employee actions. When employees engage in activities and processes, they enact existing structures which determine what is purposeful behaviour. If a new structure is introduced, it will not be organisationally integrated before the employees enact the necessary activities and processes. ISMS can be considered such a structure, which require the employee to enact its postulated activities and processes. If not, the ISMS exists only as an idealised prescription. To enable this theoretical assessment, the problem-solving methodology (M_{PS}) was created.	
Stage 2: BIE	
While the long-term plan is to make changes to NorAg's ISMS, this will be a long-drawn process containing a number of steps and stakeholders. Hence, it was not feasible to attempt to iteratively build and intervene into the ISMS as a part of this project. Instead, emphasis was directed towards the evaluation of the ISMS. More specifically, this step was dedicated to evaluating how the existing build and design of the ISMS functioned in the organisational setting. To achieve this, the M_{PS} functioned as a lens which the conducted research was analysed through. The research was initiated by applying the M_{PS} to the official ISMS documents. This led to the identification of the idealised version of the	*Applying the M_{PS} to the IT artefact:* After the problem formulation had been articulated, the documents which constitute the ISMS were reviewed once more and analysed according to the M_{PS}. This resulted in the creation of Structure #1. This structure represented the official articulation of how the ISMS at NorAg ought to function. This structure therefore served as the benchmark that opened up for evaluating how the ISMS worked in practice. With Structure #1 as a benchmark, interviews of upper management were done in order to evaluate to what extent Structure #1 represented the real

ISMS (Structure #1). This idealised version, Structure #1, made up the comparative threshold for which the subsequent structures would be identified and assessed. The subsequent structures were identified process of interviews. The interviews provided practical insight into how the various organisational units did, in fact, enact and perceive information security. This process allowed for the identification of different structures, which were not aligned with how the ISMS prescribed the alignment of information security.	conditions of the organisation and/or functioned as intended. The interviews revealed that organisational activities and processes, and the perception of these, did not match Structure #1. This led to the identification of other, prevailing structures. While a number of potential structures could be identified, there were recurring trends that allowed for the identification of four additional structures.
Stage 3: Reflection and Learning	
The research resulted in the identification of five structures: 1) Structure #1 – embodying how the ISMS is envisioned by the foundational documents. 2) Structure #2 and #3 – embody structures which prevent the ISMS from integrating into the organisation, as intended by Structure #1. 3) Structure #4 and #5 embody existing structures which offer Structure #1 an opportunity to align itself with existing activities and processes. Together, these structures demonstrate how the envisioned design of the ISMS does not correlate to the de facto conditions at NorAg.	*Assessing the problem-solving methodology (M_{PS})*: In total, eight interviews were had, which led to the creation of four additional structures, making the total amount five. The assembly of the four structures occurred through a fairly straightforward process. Each manager was interviewed with the same set of questions, in a semi-structured way. The purpose of the interviews was to identify their perception of and approach to information security. As these aspects were uncovered, they would be assessed and rephrased into a modality. After all the interviews had been conducted, a finished list of modalities had been produced. The modalities were then analysed to establish meaningful connections between the

	various modalities, resulting in the assembly of the various structures. The combination of the modalities and the assembly of these Structures were largely based on their ability to answer the Problem Formulation. Consequently, two Structures were identified to explain the challenges of ISMS alignment, and two Structures were identified to propose opportunities in aligning the ISMS.
Stage 4: Formalization of Learning	
Structure #2 and #3 elucidate a foundational problem: the ISMS is not enacted like it is envisioned by Structure #1. This becomes clear by the fact that: 1) There is a general understanding of information security as a technical problem, and 2) Information security is perceived as abstruse or removed from normal activities and processes. This indicates that the employee is not an active enactor of information security, but one which follows the communicated direction provided by the IT department. This suggests that a key obstacle to better alignment is the need to understand the existing processes and activities. By understanding these, it might be possible to introduce information security	*Assessing the problem-solving methodology (M_{PS}):* The intention for using Orlikowski's theoretical framework was for it to function as a problem-solving methodology (M_{PS}). This has occurred in two different ways: 1) If has identified factors which can inhibit the ISMS alignment. These are represented in Structure #2 and #3. 2) It has contributed to a possible solution by identifying opportunities for the ISMS to align with existing, organisational structures, as represented by Structure #4 and #5. The theoretical framework enabled a theoretical classification of activities and processes at NorAg. This classification

enactment through entrenched norms and behaviour. Structure #4 and #5 offer two versions for such alignment. These structures embodied: 1) An organisational approach to risk, and 2) An organisational focus on compliance and a recognition of GDPR as a regulation that ought to be complied with. These structures embody principles which are tightly connected to information security enactment, these structures thus provide alignment possibilities for the ISMS. The formalised learning which can be discerned from these findings are as follows: 1) Because the ISMS can be perceived to describe an idealised version of information security, organisations should analyse and understand to what extent the ISMS is functional and enacted within the organisational setting. 2) The pursuit of ISMS enactment might require structural changes within the organisation.	opened for making connections which otherwise might not have been discernible. This provided a deeper insight into the recursive relationship between information security, as a structure, and the employee, as an agent.

3.5.3 The Problem-solving Methodology (M_{PS})

Giddens maintained that '*the modalities of structuration are drawn upon by actors in the production of interaction*' while simultaneously being the '*media of the reproduction of the structural components of systems of interaction*' (Giddens 1979, p. 81). It is recognised that all human interaction intrinsically contains these modalities, which fuses the sphere of social action with that of structure (Giddens 1979) (Giddens 1984) (Orlikowski and Robey 1991, p. 148). Due to this, Giddens has considered that all interaction between action and structure can be analysed in terms of these modalities (Orlikowski and Robey 1991, p. 148). Orlikowski built on this and created a lens which she used to identify and assess the empirical manifestations of these modalities (Orlikowski 2000). Inspired by this, the theoretical lens has been repurposed to study information security alignment.

When an employee acts either in accordance with or contrary to an organisation's specified IT artefact, which in this study is represented by the ISMS, they draw on three different forms of properties which constitute the IT artefact (Orlikowski 2000):

1) The functionalities and boundaries contained within the IT artefact (technologies, mechanisms, practices, etc.);
2) Those inscribed by the designers (the policies and guidelines articulating the nature of the IT artefact in the organisation);
3) The habits created by employees which have interacted with the IT artefact up to the present point;
4) In addition, the individual will draw on their skills, knowledge, expectations, assumptions and context (Orlikowski 2000).

This indicates that there are a number of sources that can influence how employees engage with IT artefacts. However, a group of employees which work together conduct similar activities and processes tend to engage with IT artefacts the same way (Orlikowski 2000, p. 411). The influence of group practices has proven to be able to override the use intended by the designers and even reduce the impact of the functionalities with the IT artefact (Orlikowski 2000, p. 411). This type of rigid group dynamic can, thus, prevent employees from enacting IT artefacts as intended (Orlikowski 2000). Following this logic, the successful alignment of an organisation's ISMS across the organisation would be impacted by existing group dynamics. That is not to say, however, that group dynamics are permanently fixed. There is a variety of factors that can enable changes in the enactment of IT artefacts, such as new training or policies (Orlikowski 2000). Such interventions would, however, hinge on the awareness and understanding of these dynamics. The purpose for using the lens provided by Orlikowski is to identify and map existing dynamics within an organisation. This allows for the analysis and assessment of how existing structures coincide or contradict the envisioned enactment of the ISMS.

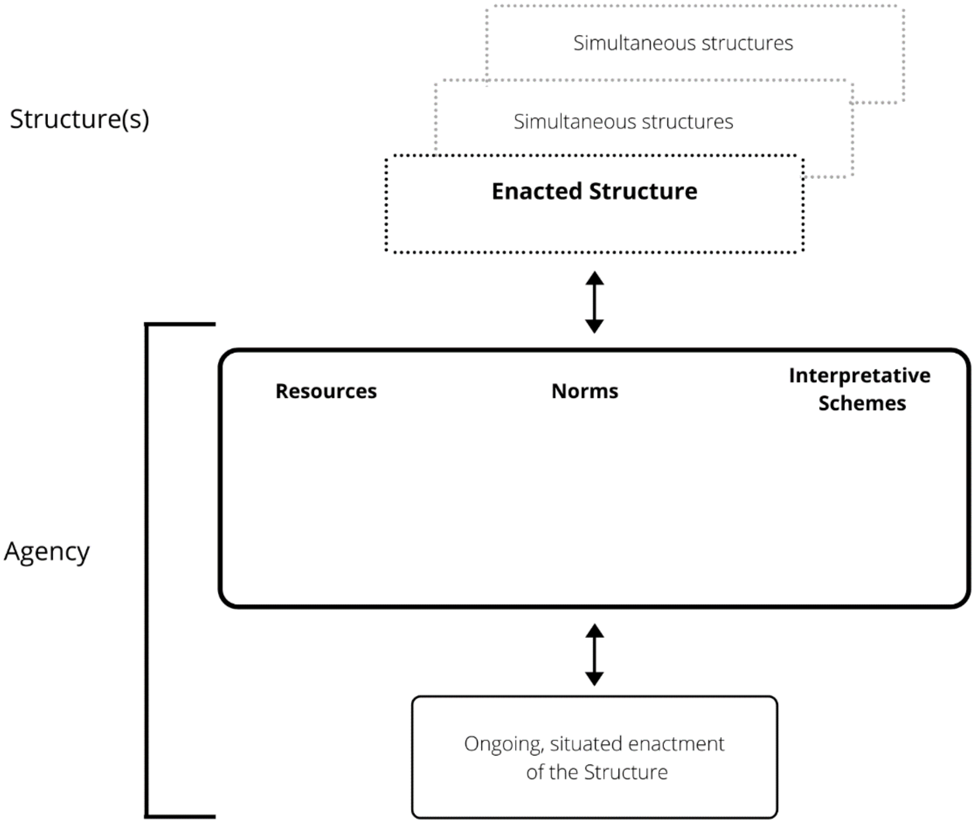


Figure 3.6 – The Problem-solving Methodology – Structuration

Derived from Orlikowski (Orlikowski 2000)

3.6 Data Collection

Two types of data collection have occurred throughout this project, and the two different forms have been used for two different purposes.

3.6.1 Document Reviews

The thesis topic emerged from an agreement with the information security team. This was, however, merely a discursive beginning. To properly initiate the thesis and precisely formulate the problem, found documents from the organisation were utilised as a starting point to create the epistemological foundations for the thesis. By found documents it is meant documents (including multimedia documents such as other visual, aural or electronic media) which have been produced by or for the organisation (Oates 2005, pp. 233-235). Full access was provided to classified information security documents, and wide access to organisational documents was already enjoyed due to the researcher’s employment at the organisation. Because all the documents originated from the organisation, it was not necessary to study their reliability. There were primarily two classifications of documents which were used:

1) Organisational documents about information security intended for the whole organisation. This included documents on information security policies; data classification; incident response; crisis management; and security updates on the intranet, to mention only some of the sources. This was also complimented by more general documents regarding the organisation as a whole.
2) Documents specific to those involved with information security. This included security audits; gap and maturity assessments; asset registers; and incident reports, to mention only some types of documents. A number of these were classified and only accessible for the information security team and upper management.

These documents were then systematically read and analysed. Together, they provided the official description of how the ISMS should be enacted at NorAg. By applying the M_{PS} to the documents, Structure #1 was created.

3.6.2 Semi-structured Interviews

The document review provided the epistemological foundations of the thesis and allowed for the building of Structure #1. The next step was to evaluate the validity Structure #1, as the official vision of the ISMS. This was achieved through the use of interviews.

Interviews were utilised for two reasons in particular:

1) First of all, because the researcher was employed at the organisation, the researcher was already familiar with the people and the culture. This enabled the interviews to be done with significant trust, honesty and mutual understanding (Oates 2005, pp. 186-191), giving the interviews considerable elucidating potential. Additionally, because the researcher was already situated in the organisation, it was a notably low threshold to gain access to upper management.
2) Secondly, the documents concerned with the organisational perspective on information security provided the formalised postulations of the organisation. Through interviews, however, it was possible to explore and discover the de facto perceptions of the upper management. Because the purpose was to elucidate perspectives which were not evident from the formalised information, semi-structured interviews were employed to enable the interviewees to share their perspectives inside a flexible format (Oates 2005, p. 188).

The upper management at NorAg were the focus of the interviews. There were two reasons for this:

1) As previously defined, the role of the management is to articulate, motivate and direct the fulfilment of strategic goals and objectives. Management is therefore identified as a key driver in the maintenance or change of social systems within the organisation. Understanding how management experiences information security is, therefore, arguably a vital perspective.
2) Due to limitations in time of the study and the complexity of NorAg, it was not feasible to interview a representative number of employees from the various units. While the upper management inevitably is further removed from the daily activities and processes, their role ought to require insight into these activities and processes. Hence, upper management was considered to offer more representative insights into the organisational dynamics.

The upper management that were interviewed were identified through the official, organisational structural overview which is available both externally and internally. The regional office manager was selected based on the knowledge that the person had extensive leadership experience from NorAg. The organisational security manager was identified and selected due to the person's involvement in the overarching, organisational security.

3.6.3 Overview of Interviewees

Table 3.6 – Interviewees

No.	Role	Responsibilities	Offered insights
5 + 1	Upper management + A representative of an upper manager	Responsible for organisational strategy. Responsible for organisational divisions. Responsible for divisional strategies and divisional functions.	An overarching and holistic view of information security seen in context of the organisation's strategies, activities and challenges.

1	Regional office manager	Responsible for the management of a regional office representing a region outside of Europe.	A narrowed down view of information security as required and/or enacted 'on the ground'.
1	Organisational security manager	Responsible for organisational security, risk management and crisis management across the organisation.	A broad perspective on the general preparedness and security practices of the organisation.

4. Findings

The first step of the thesis consisted of articulating the practical problem formulation. When the problem was encapsulated, the next step was to find the adequate academic approach to the problem. This was done by employing structuration theory, and Orlikowski's theoretical lens, as the epistemological framework. This framework provided the theoretical concepts which enabled the inquiry that was conducted. Due to the central role of the framework in both identifying and analysing ISMS alignment factors, the framework was categorised as a problem-solving methodology, according to suggested practice by McKay and Marshall (McKay and Marshall 2007). The problem-solving methodology has functioned as a theoretical lens which allowed for the identification of existing structures at NorAg. The purpose of the problem-solving methodology has been to uncover new knowledge about ISMS alignment at NorAg. As a theoretical framework in Action Design Research, following the FMA logic, it has also provided an academic rigidity that ought to ensure the recoverability of the research and analysis.

The problem-solving methodology, as a lens ready for input, is illustrated in Figure 3.6. This was first put to the test by applying it to the document reviews, in the initial phase of the research. The foundational properties of NorAg's official ISMS have been summarised in Table 4.1. Due to the sensitivity of the topic, these properties are the summarised and generalised aspects of the ISMS, processed to be suitable for external readers. This created Structure #1, representing the official postulation and expectation of how the ISMS ought to be integrated and enacted at NorAg. This structure would then serve as the benchmark for the subsequent interviews which were made. The purpose of these interviews was to evaluate the validity of

Structure #1, and to identify potential discrepancies. These discrepancies were, in general, identified when an interviewee described an activity, process or sentiment which contradicted the official ISMS. As discrepancies were uncovered, these were categorised as different types of modalities of structuration, which were fitted into the problem-solving methodology. As new modalities were uncovered, new structures which impacted how the ISMS was integrated and enacted were identified. In total, five structures were identified. It must be noted that more structures could be identified, based on the data gathered from the interviews. However, due to the limited scope, the once which were considered the most decisive and universal were selected.

Table 4.1 – Properties of NorAg's ISMS

Properties of NorAg's ISMS	
Elements	**Properties**
Principles (employees)	Every employee is considered a decision-making agent regarding information security. They are therefore to be considered responsible for their own security compliance in their system and information use.
Principles (top management)	The top management should demonstrate their commitment by recurrently discussing and ratifying the principal information security policy, thereby ensuring the constant dissemination of the importance of said policy across the organisation. Top management will create the necessary corporate culture and context for security compliance.
Policies	The policies define the objectives, strategies and organisation of the information security, and outline the information security governance framework. The most central policies are: - The principal information security policy - IT assets (software and hardware) policy - Access control - Mobile devices policy - Privacy policy
Routines and Standards	Documented routines will guide and facilitate compliance with the information security.

Awareness and education	Available information and training will inform employees about their responsibilities regarding information security, increasing their awareness of risks and consequences, and leading to informed decisions on security.
Roles and responsibility	The responsibility for information security compliance has been spread across key roles. This includes, but is not limited to, the information and risk owners; the information user; and the top management. The purpose is to ensure that the strategies and objectives of the ISMS is implemented and integrated across the organisation.
IT Infrastructure / Technical Controls	IT will ensure that the security of the IT infrastructure is maintained. The security controls will be proportionate to the risk and support organisational objectives. There is an intent to reduce restrictive, preventative controls.

4.1 People Centric Security – Structure #1 (Official ISMS)

Digital transformation has been a large focus of NorAg over the past years. The development of the ISMS has mirrored that. The ISMS is therefore comprehensively described, with the information readily available to all employees. These documents, which make up the blueprint of the ISMS, describes the intended state of the information security at NorAg. Through a document review, this intended state has been fitted into Orlikowski's lens, creating Structure #1, as demonstrated in Figure 4.1.

Structure #1

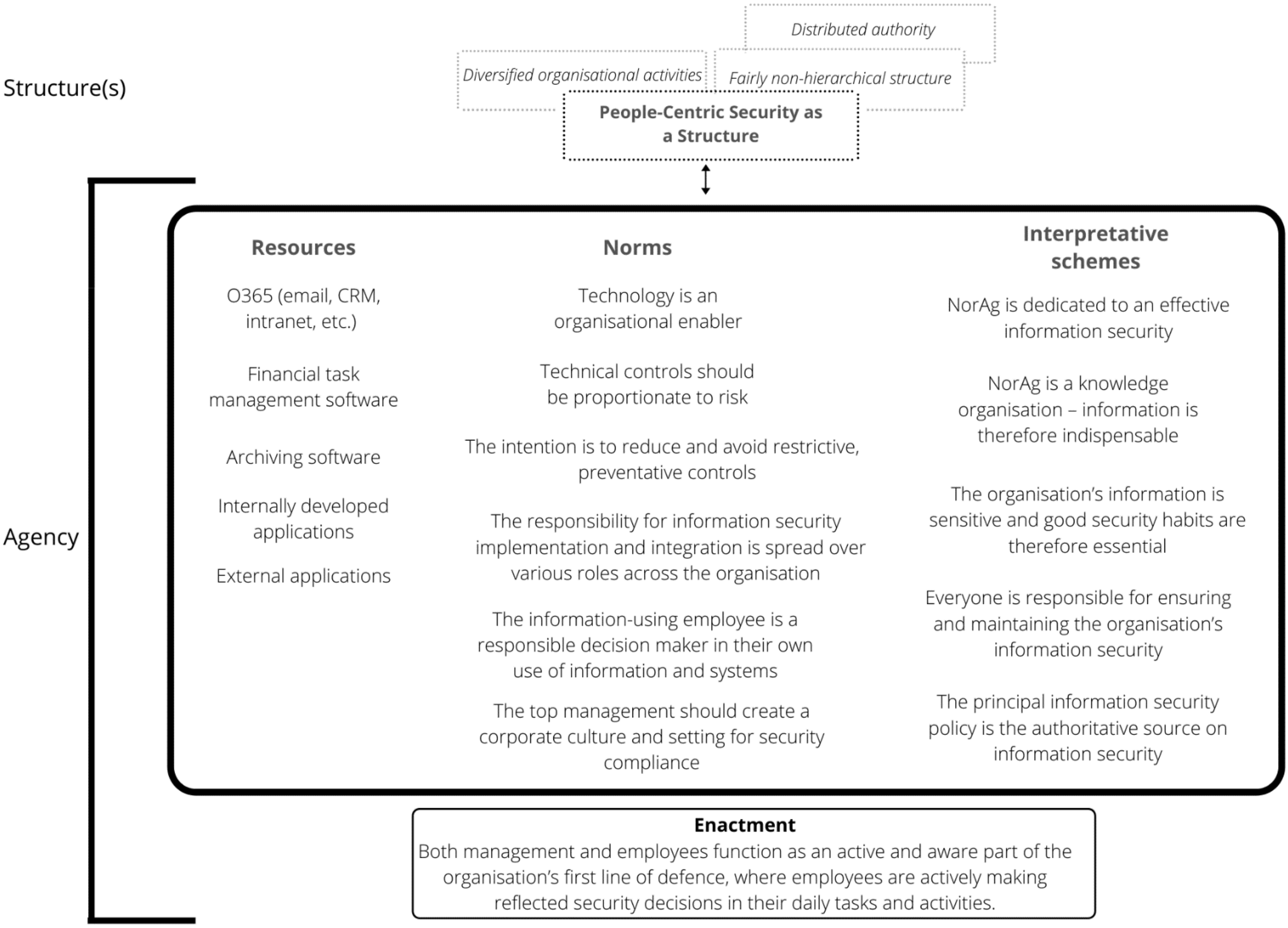

Structure(s)
Distributed authority
Diversified organisational activities
Fairly non-hierarchical structure
People-Centric Security as a Structure
Agency
Resources
O365 (email, CRM, intranet, etc.)
Financial task management software
Archiving software
Internally developed applications
External applications
Norms
Technology is an organisational enabler
Technical controls should be proportionate to risk
The intention is to reduce and avoid restrictive, preventative controls
The responsibility for information security implementation and integration is spread over various roles across the organisation
The information-using employee is a responsible decision maker in their own use of information and systems
The top management should create a corporate culture and setting for security compliance
Interpretative schemes
NorAg is dedicated to an effective information security
NorAg is a knowledge organisation – information is therefore indispensable
The organisation's information is sensitive and good security habits are therefore essential
Everyone is responsible for ensuring and maintaining the organisation's information security
The principal information security policy is the authoritative source on information security
Enactment
Both management and employees function as an active and aware part of the organisation's first line of defence, where employees are actively making reflected security decisions in their daily tasks and activities.

Figure 4.1 – Structure #1

Table 4.2 – Structure #1 Summarised

Structure #1 Summarised	
Structure	The ISMS is marked by a People-Centric Security (PCS), indicating that employees are empowered and enabled to be making autonomous security decisions (Levy 2015).
Parallel Structure(s)	The PCS is occurring in parallel with at least three other structures affecting it:

	1) *Diversified organisational activities* – the forms of services provided are multitude; the customers are diverse; the geographical reach is wide; and the assignments are many. This leads to a complex organisation where the types of activities and IT assets used is difficult to pinpoint. 2) *Distributed authority* – due to the variety in organisational activities and assignments, decision-making power has been distributed across the organisation. 3) *Fairly non-hierarchical structure* – although there is officially an organisational hierarchy, the structure is characterised by a distinct flatness. The relationships between employees and managers are built on mutual trust.
Resources	There is a constant bundle of IT assets used by the vast majority of the organisation included in O365. It is also a team responsible for developing new solutions. Additionally, a variety of external applications are also used.
Norms	The norms emanate from the postulation that the ISMS has a flexible focus on supporting the objectives of the organisation. The employee is therefore, through their behaviour and decisions, considered an important part of enacting everyday security. The top management is identified as establishing the setting and culture which leads to security compliance.
Interpretative schemes	The ISMS is founded on the stock of knowledge which identifies information as a crucial aspect of NorAg. It is therefore expected that this awareness is shared by all employees, and the path to compliance is provided by the information security policies, and through additional training and information.

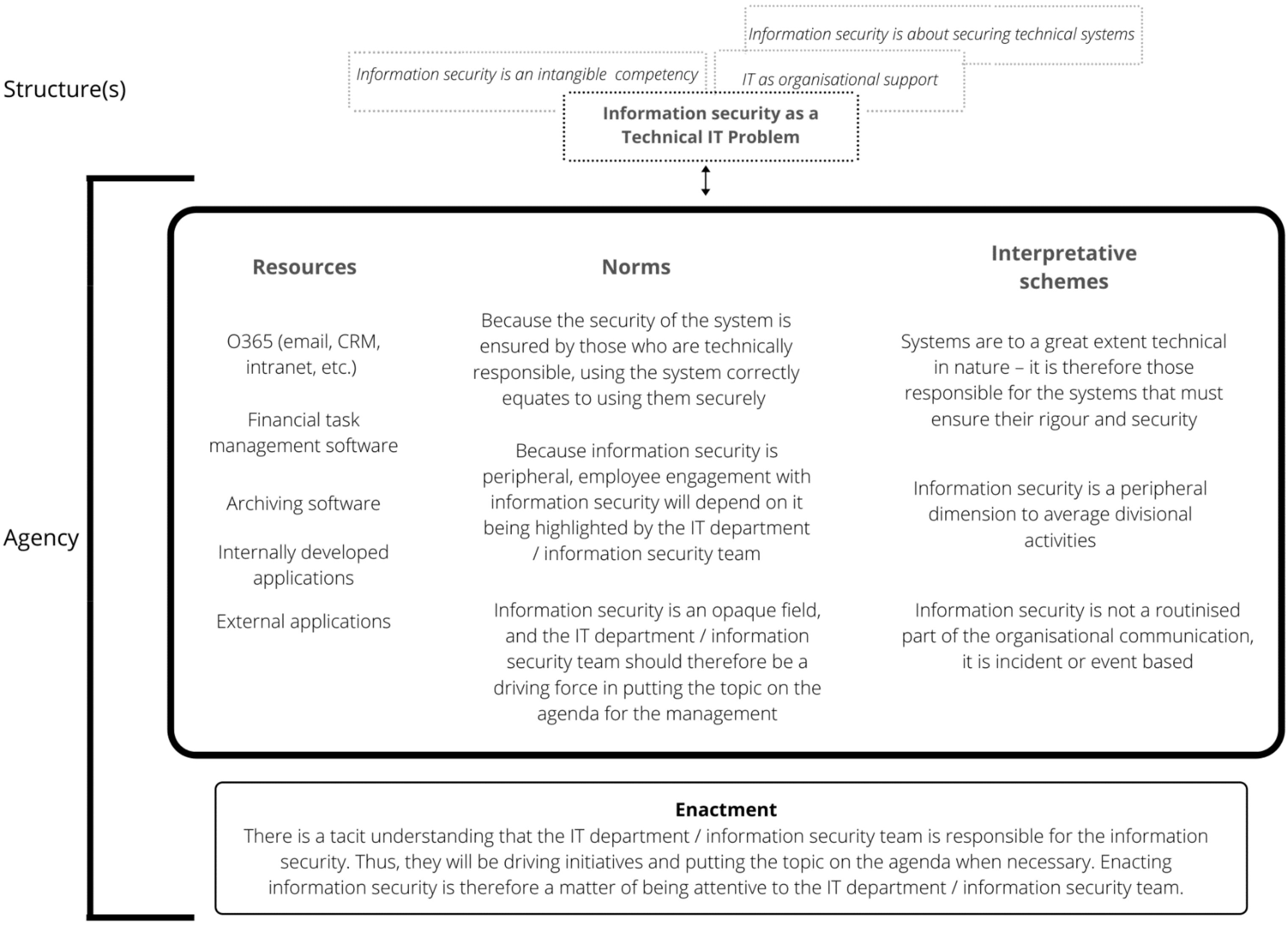
Structure #1 represents the ideal vision of the ISMS, because it is not based on empirical conditions, but serves as a prescriptive framework for the organisation.

4.2 Structures Hampering Information Security

Through the interviews, a variety of modalities were indirectly described. While this would enable the identification of a variety of structures which appeared to obstruct the ISMS integration, there were two structures in particular which appeared more decisive than others. Due to the limited scope of the study, these two were given precedent.

4.2.1 Information Security as a Technical IT Problem

Structure #2



Structure(s)

Information security is about securing technical systems

Information security is an intangible competency

IT as organisational support

Information security as a Technical IT Problem

Agency

Resources

O365 (email, CRM, intranet, etc.)

Financial task management software

Archiving software

Internally developed applications

External applications

Norms

Because the security of the system is ensured by those who are technically responsible, using the system correctly equates to using them securely

Because information security is peripheral, employee engagement with information security will depend on it being highlighted by the IT department / information security team

Information security is an opaque field, and the IT department / information security team should therefore be a driving force in putting the topic on the agenda for the management

Interpretative schemes

Systems are to a great extent technical in nature – it is therefore those responsible for the systems that must ensure their rigour and security

Information security is a peripheral dimension to average divisional activities

Information security is not a routinised part of the organisational communication, it is incident or event based

Enactment

There is a tacit understanding that the IT department / information security team is responsible for the information security. Thus, they will be driving initiatives and putting the topic on the agenda when necessary. Enacting information security is therefore a matter of being attentive to the IT department / information security team.

Figure 4.2 – Structure #2

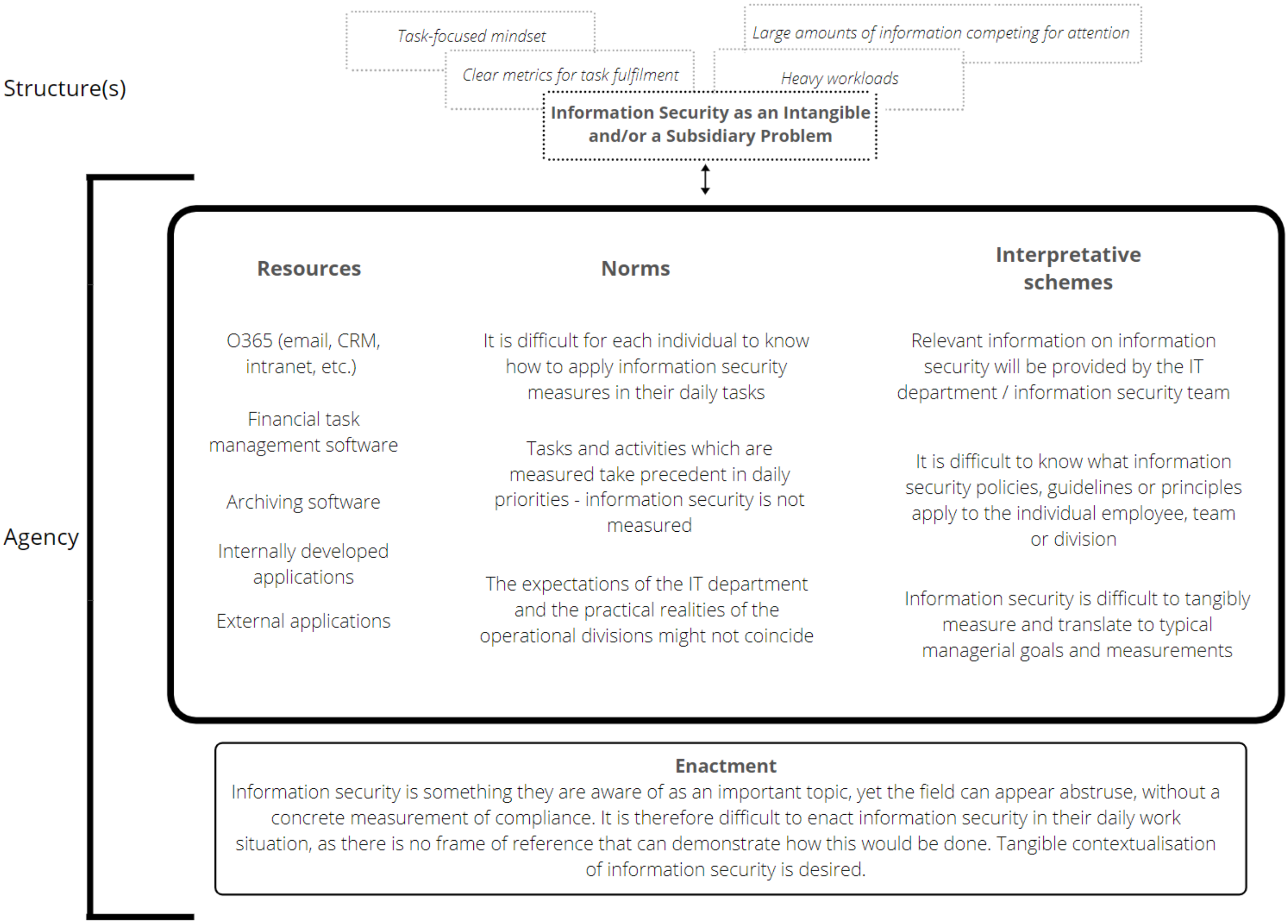
Table 4.3 – Structure #2 Summarised

Structure #2 Summarised	
Structure	Information security is intrinsically linked to digital tools (IT assets) of which the IT department has the technical responsibility for. The technical capacities of the IT department, and their information security team, is therefore considered the first line of defence.
Parallel Structure(s)	This structure is occurring in parallel with at least three other structures affecting it: 1) *IT as organisational support* – the IT department is considered both responsive and capable at addressing the IT-related issue experienced by all employees. Moreover, the threshold of getting in touch with them is low. There is therefore an implicit understanding that IT has an authoritative, technical responsibility. 2) *Information security is about securing technical systems* – if the IT asset (application, hardware, solution, etc.) is configured correctly, then it is considered to be adequately protected. 3) *Information security is an intangible competency* – due to its technical association, and its propensity to contain complex terminology, information security competence can appear difficult to attain for those outside of the field.
Resources	There is a constant bundle of IT assets used by the vast majority of the organisation included in O365. It is also a team responsible for developing new solutions. Additionally, a variety of external applications are also used.
Norms	The norms emanate from a reliance of the IT department as a technical authority. Because information security is perceived a technical issue, there is a certain expectation that the user of

	IT assets does not have a decisive and active part in enacting information security. Their enactment happens primarily through the correct use of the technical IT assets. This also means that the security behaviour is initiated and moulded by directions provided by the IT department, and not by initiatives and decisions made by the average employee.
Interpretative schemes	Because the main source of communication on information security is the IT department, there is a presiding perception that the IT department is the arbiter of knowledge about information security.

4.2.2 Information Security as a Subsidiary and/or Peripheral Problem

Structure #3


Structure(s)
Task-focused mindset
Clear metrics for task fulfilment
Large amounts of information competing for attention
Heavy workloads
Information Security as an Intangible and/or a Subsidiary Problem
Agency
Resources
Norms
Interpretative schemes

O365 (email, CRM, intranet, etc.)

Financial task management software

Archiving software

Internally developed applications

External applications

It is difficult for each individual to know how to apply information security measures in their daily tasks

Tasks and activities which are measured take precedent in daily priorities - information security is not measured

The expectations of the IT department and the practical realities of the operational divisions might not coincide

Relevant information on information security will be provided by the IT department / information security team

It is difficult to know what information security policies, guidelines or principles apply to the individual employee, team or division

Information security is difficult to tangibly measure and translate to typical managerial goals and measurements

Enactment

Information security is something they are aware of as an important topic, yet the field can appear abstruse, without a concrete measurement of compliance. It is therefore difficult to enact information security in their daily work situation, as there is no frame of reference that can demonstrate how this would be done. Tangible contextualisation of information security is desired.

Structure #3 Summarised	
Structure	Information about the risks associated with information security is readily available both internally from the organisation, and externally from the media. There is therefore a widespread awareness that information security is important. However, the discourse on information security can appear abstruse and/or convoluted. This makes it difficult to understand how information security can be enacted in normal, divisional operations.
Parallel Structures	This structure is occurring in parallel with at least four other structures affecting it: 1) *Task-focused mindset* – NorAg is a fairly complex organisation with a wide variety of activities and processes. Employees often have a variety of both short-term and long-term tasks and projects which they need to fulfil. Employees can therefore experience limited opportunities to engage with topics which do not appear directly related to what they normally do. 2) *Clear metrics for task fulfilment* – NorAg has a comprehensive structure and culture for documenting, reporting on, and measuring results. Measured tasks hence take a precedent in the normal workday. 3) *Heavy workloads* – There are clear expectations to both operational efficiency and cost-efficiency. Workloads are therefore, in general, high. 4) *Large amounts of information competing for attention* – while the activities and processes are notably diverse, there is a stated desire for more cross-organisational cooperation. This leads to an abundance of available information on the intranet and associated channels. This means that it can be difficult to break through with information.
Resources	There is a constant bundle of IT assets used by the vast majority of the organisation included in O365. It is also a team responsible for developing new solutions. Additionally, a variety of external applications are also used.

Norms	The norms emanate from a perception that information security is abstruse and often inadequately contextualised. The normal workday is filled with both short-term and long-term tasks whereof results are measured. Additionally, there is a number of other activities and processes happening simultaneously which also strive for cross-organisational attention. The information provided on information security might, therefore, not make the necessary impact on the individual employee.
Interpretative schemes	NorAg has an important position both for Norwegian businesses in particular and society in general. There is therefore a strong sense of what one ought to achieve and how efficiently one ought to do it. This limits an employee's capacity to familiarise themselves with topics which do not appear directly relatable. This is further bolstered by a metric and result driven culture.

4.3 Structures Which Potentially Align with Information Security

The past section listed two structures which can impede on the organisational integration of information security. This section has, on the other hand, identified two existing structures which can enable for better information security alignment. These structures already exist within the organisation. Of these, one of them is not directly concerned with information security. This is a structure concerned with organisational risk, which encompasses all forms of risks faced by the organisation. This is a well-established structure which enjoys considerable support and understanding in the organisation. The second takes on more of a budding state. This structure represents the general awareness and acceptance of GDPR as an important regulation which must be complied with. Although it enjoys a wide recognition, it is budding because there's no tangible understanding of how to best apply it in the various, divisional activities and processes.

4.3.1 Organisational Risk and Compliance as a Structure

Structure #4

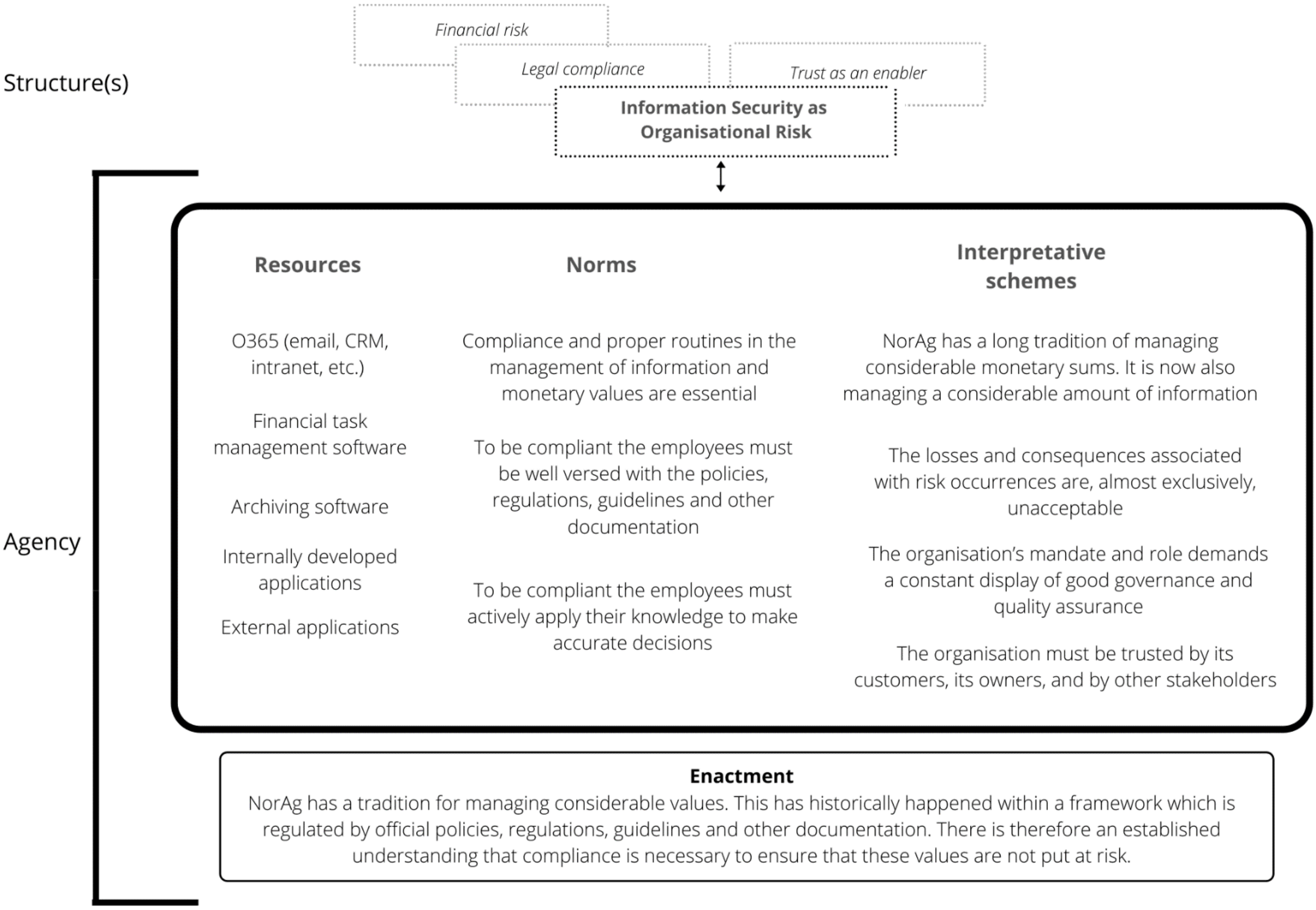

Structure(s)
Financial risk
Legal compliance
Trust as an enabler
Information Security as Organisational Risk
Agency
Resources
Norms
Interpretative schemes
O365 (email, CRM, intranet, etc.)
Financial task management software
Archiving software
Internally developed applications
External applications
Compliance and proper routines in the management of information and monetary values are essential
To be compliant the employees must be well versed with the policies, regulations, guidelines and other documentation
To be compliant the employees must actively apply their knowledge to make accurate decisions
NorAg has a long tradition of managing considerable monetary sums. It is now also managing a considerable amount of information
The losses and consequences associated with risk occurrences are, almost exclusively, unacceptable
The organisation's mandate and role demands a constant display of good governance and quality assurance
The organisation must be trusted by its customers, its owners, and by other stakeholders
Enactment
NorAg has a tradition for managing considerable values. This has historically happened within a framework which is regulated by official policies, regulations, guidelines and other documentation. There is therefore an established understanding that compliance is necessary to ensure that these values are not put at risk.

Figure 4.4 – Structure #4

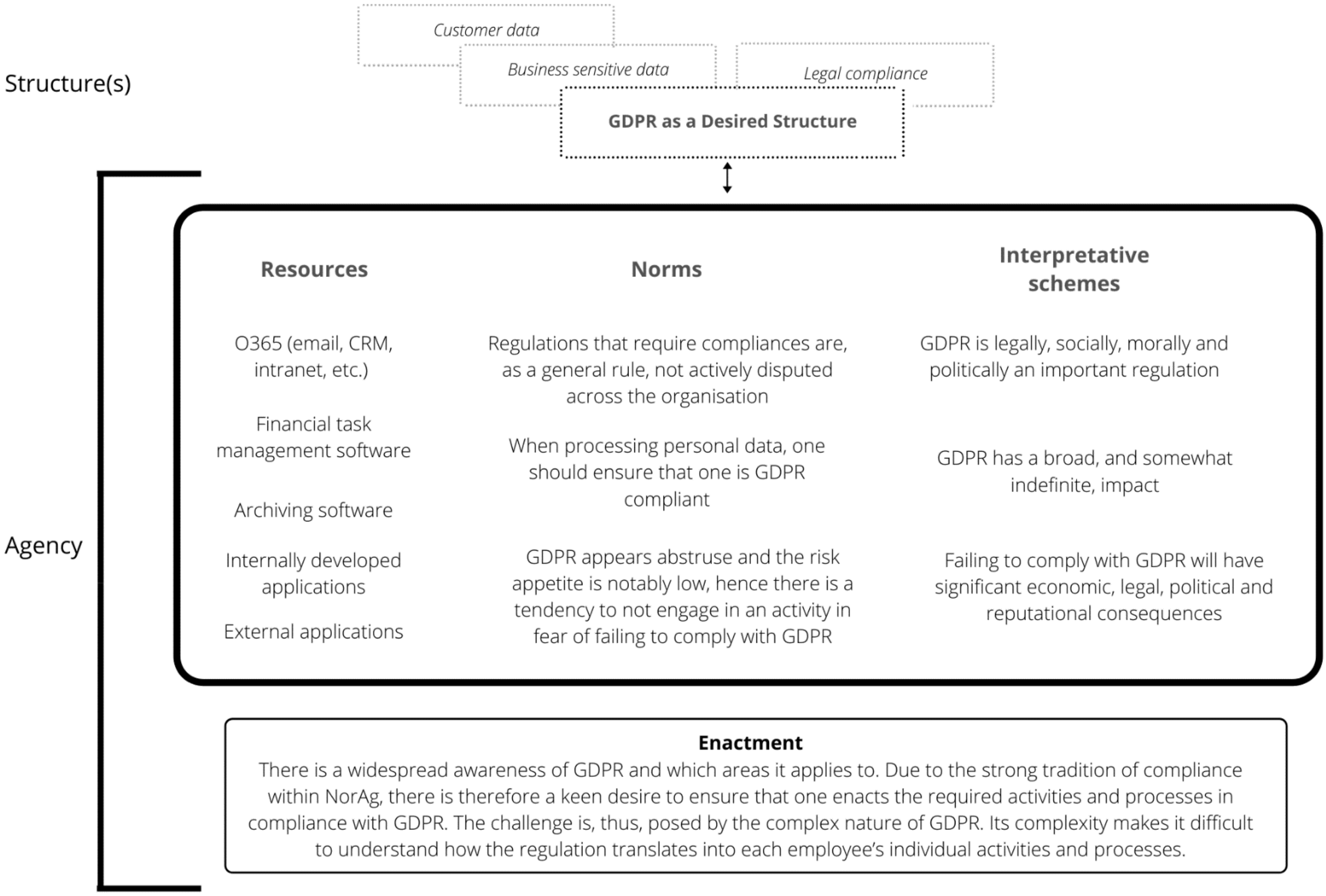
Table 4.5 – Structure #4 Summarised

Structure #4 Summarised	
Structure	NorAg has an established tradition for managing considerable monetary sums. Moreover, it has a deeply entrenched recognition of the responsibility this entail for their customers, owners and other stakeholders. There is therefore an acceptance that policies, regulations, guidelines and other organisational rigidities are necessary to ensure good governance, quality assurance and compliance.

Parallel Structure(s)	There are three other structures which simultaneously bolster this: 1) *Financial risk* – NorAg has the staff, structure, agreements, competency and awareness for securely managing considerable monetary values. 2) *Legal compliance* – NorAg has the staff, structure, competency and awareness that ensures that a complex compliance regime does not impede on its ability to operate according to its organisational objectives. 3) *Trust as an enabler* – NorAg is a public organisation, and its licence to operate is therefore determined by its ability to responsibly live up to the trust it receives from both society and state. Without this trust, NorAg will not be able perform its mandate.
Resources	There is a constant bundle of IT assets used by the vast majority of the organisation included in O365. It is also a team responsible for developing new solutions. Additionally, a variety of external applications are also used.
Norms	The norms emanate from an established understanding of compliance as necessary to achieve the foundational organisational objectives. There is hence an established recognition that daily tasks and activities will have to be enacted while complying with necessary policies, regulations and guidelines.
Interpretative schemes	The avoidance of organisational risk is considered a fundamental enabler of NorAg's mandate to operate. The necessity for compliance is therefore not questioned. Instead it is accepted and deeply integrated, to the extent that the knowledge of how to be compliant, and the purpose it serves, is nearly ubiquitous.

4.3.2 GDPR as a Desired Structure

Structure #5


Structure(s)
Customer data
Business sensitive data
Legal compliance
GDPR as a Desired Structure
Agency
Resources
Norms
Interpretative schemes
O365 (email, CRM, intranet, etc.)
Financial task management software
Archiving software
Internally developed applications
External applications
Regulations that require compliances are, as a general rule, not actively disputed across the organisation
When processing personal data, one should ensure that one is GDPR compliant
GDPR appears abstruse and the risk appetite is notably low, hence there is a tendency to not engage in an activity in fear of failing to comply with GDPR
GDPR is legally, socially, morally and politically an important regulation
GDPR has a broad, and somewhat indefinite, impact
Failing to comply with GDPR will have significant economic, legal, political and reputational consequences
Enactment

There is a widespread awareness of GDPR and which areas it applies to. Due to the strong tradition of compliance within NorAg, there is therefore a keen desire to ensure that one enacts the required activities and processes in compliance with GDPR. The challenge is, thus, posed by the complex nature of GDPR. Its complexity makes it difficult to understand how the regulation translates into each employee's individual activities and processes.

Figure 4.5 – Structure #5

Table 4.6 – Structure #5 Summarised

Structure #5 Summarised	
Structure	GDPR is represented both formally and informally. Formally it is represented by organisational policies, regulations and guidelines asserting the importance of GDPR in NorAg.

	Informally it is displayed in the general, cross-organisational awareness held by the employees.
Parallel Structure(s)	There are three other structures which simultaneously bolster this: 1) *Legal compliance* – NorAg has the staff, structure, competency and awareness that ensures that a complex compliance regime does not impede on its ability to operate according to its organisational objectives. 2) *Customer data* – NorAg is both a data controller and data processor, managing substantial amounts of customer data. The governance of this customer data is a subject of continuous discourse on all levels of the organisation. 3) *Business sensitive data* – there is foundational awareness that a considerable amount of the data owned by NorAg is highly sensitive for the relevant businesses.
Resources	There is a constant bundle of IT assets used by the vast majority of the organisation included in O365. It is also a team responsible for developing new solutions. Additionally, a variety of external applications are also used.
Norms	There is a widespread acceptance of and desire to comply with GDPR. There is, hence, an established recognition that information security is, if indirectly through compliance of a privacy regulation, an important factor that has the authority to change organisational activities and processes.
Interpretative schemes	There is an intrinsic understanding that GDPR is highly relevant to NorAg due to the types of data which the organisation controls and processes. There is a desire to comply with the regulation because there is a general agreement that the consequences for not doing it is unacceptable.

5. Discussion

The duality of structure describes the reciprocal process where human action creates the structural properties of a social system, which in turn goes on to shape human action. In organisational life, these self-reinforcing feedback loops arguably materialise in activities and processes which are enacted to achieve the organisational objectives. When an employee enters an organisation, they enter already existing structures which inform them what type of behaviour is purposeful. Yet, the employee can simultaneously shape this structure. They can, for example, change it by introducing new technologies or new knowledge. Yet, attempts at changing the structure might also be met with opposition by other employees who enact it. When seeking to introduce new structures, with new activities and processes, to an organisation, it is, thus, imperative to identify and understand the current structures, together with their pertinent activities and processes.

With structuration theory as the epistemological foundation of this thesis, an underlying assumption has been that the alignment of information systems requires a process of structuration to occur. Situated within the context of this paper, the assumption has been that the alignment of information security, embodied by the ISMS, into an organisation will require such a process. Information security is, for the vast majority of organisations, extrinsic to their core activities. The integration of the ISMS will therefore appear like the introduction of a new structure into an organisation. Inevitably, this will lead to a situation where the new information security structure(s) encounters the presiding structures of the organisation. The existing structures can either serve as obstacles for the processes of structuration to occur, or it can enable the necessary processes to take place.

In this thesis, it is assumed that for information security is most effective when it is integrated into the normal activities and processes across the organisation. Hence, if the already existing structures appear as obstacles in the introduction of information security structures, this means that they will negatively impact the extent to which information security is integrated across the organisation. And, conversely, if the presiding structures allow for the introduction of the structures of information security, it will enable the necessary alignment. Understanding the existing structures of an organisation is therefore key to assessing and understanding the possible success of information security alignment. This has been sought achieved by employing a theoretical framework developed by Wanda Orlikowski as a problem-solving methodology. By utilising this framework, the intention has been to understand how information security can or cannot align with structures which are already in place.

In total, five structures were identified. Of these, Structure #1 was an ideal version, as articulated by the formal ISMS documents. This represents NorAg's intention for what their information security ought to look like. This structure functioned as the benchmark for which the four subsequent structures were identified and assessed. Two of the structures, discussed below in 5.1, went in opposition to Structure #1. The remaining two structures, discussed below in 5.2, offered opportunities for aligning information security with existing dynamics.

5.1 People-Centric Security as a Structure (Official ISMS) – Structure #1

Structure #1 represents the state of the information security at NorAg as described by its ISMS documentation. It describes the optimal condition of how information security ought to be integrated in NorAg. This structure envisions information security as being deeply ingrained in both the Norms and Interpretative schemes of the organisation. The stock of knowledge in the organisation declares information security as essential to the organisational activities, processes and objectives. This is possible to assert because of the importance which is attached to the information managed by NorAg. The enactment of this is discernible by each employee demonstrating their commitment to information security by being informed about the topic and making responsible decisions in their daily activities and processes.

5.2 Opposing Structures – Structure #2 and #3

Structure #2 and Structure #3 demonstrated notable contradictions to Structure #1 and were therefore considered to be working against the vision described by Structure #1.

5.2.1 Information Security as a Technical IT Problem – Structure #2

Structure #2 represents a dynamic where information security is perceived as a technical IT problem. This structure identifies the activities and processes which are associated with enforcing the information security at NorAg to be largely limited to the domain of the IT department. The role of the individual employee is to correctly use the available information systems and be attentive to information provided by the IT department. The Norms of this structure, thus, catalogue a receptive, yet passive, employee, and an active and fully responsible IT department. These norms are based in stocks of knowledge which views information security as technical systems, rather than socio-technical systems. This assumption leads to the perception that securing the technical systems makes up a predominant segment of information security. As this segment is largely restricted to the IT department, information security integration across the organisation does not necessarily appear like a pressing, organisational endeavour.

5.2.2 Information Security as a Subsidiary and/or Peripheral Problem – Structure #3

Structure #3 represents a dynamic where information security is perceived as abstruse. This signifies that the employee does not have sufficient knowledge or competency to relate information security to their normal activities and processes. Furthermore, because the enacting of information security principles is not tangibly measured, it is experienced as difficult to evaluate how it is being enacted and the potential impact of the enactment. This is in contrast to the organisational activities and processes which are clearly defined by the organisational Norms. Moreover, how these activities and processes should be enacted and how they will be measured is also made clear by the dominant stock of knowledge which puts an emphasis on achieving measurable results. Information security does not have the same, clear representation of how it ought to be enacted, how it will be measured, and the importance of such measurement.

5.3 Potentially Aligning Structures – Structure #4 and #5

Structure #4 and Structure #5 demonstrated modalities where there were discernible overlaps with the modalities prescribed by Structure #1. These, therefore, offer potential opportunities for introducing principles from information security into already existing structures.

5.3.1 – Organisational Risk and Compliance as a Structure – Structure #4

Structure #4 represents an existing dynamic where there is a notable attention to risk, and an active effort in ensuring that risk is carefully managed. While the desire to carefully manage risk is not an uncommon trait of an organisation, the extent to which it is entrenched into the organisational objectives is notable. The Norms, which describe how the activities and processes must be compliant, are clearly described in official documentation and frequently reiterated in both informal and formal communication inside NorAg. These are founded on a stock of knowledge which declares risk mitigation as crucial for its permission and ability to achieve its organisational objectives. Hence, although compliance functions as an auxiliary function, it has been integrated as it would be a main objective.

5.3.2 – GDPR as a Desired Structure – Structure #5

Structure #5 does not, per say, represent dynamics which is currently enacted. There is a general uncertainty about how GDPR is supposed to be enacted across the organisation, and there are therefore no discernible Norms which support the activities and processes. Nonetheless, it is a widespread attentiveness and desire to correctly enact GDPR. No other topics within the field of information security (considering privacy to belong to the field of information security) received the same amount of mentions in the conducted interviews. Hence, it can be said that there is a desire for a GDPR structure to be tangibly implemented. The employees are arguably requesting new modalities of structuration to inform the new activities and processes. This is founded on a stock of knowledge which declares GDPR as highly relevant and important for NorAg. Furthermore, the employees seem to have readily adopted this awareness, and realised the potential consequences of the failure to adjust their activities and processes according to GDPR. This demonstrates that NorAg is ready to accept regulations related to information security not merely as a 'tick-the-box exercise', but as pivotal to organisational objectives.

5.4 – Summarising the Structures

The problem formulation asserted that the ISMS at NorAg was not adequately integrated into the organisational activities and processes across the organisation. As a result, information security remained predominantly the responsibility of the IT department. This went contrary to NorAg's ISMS, represented by Structure #1, which declared that information security is the active responsibility of everyone in the organisation. It should not be limited to the IT department. Structure #2 and #3 served to demonstrate that there is a discrepancy between how information security is articulated by the ISMS, and how it is perceived in the other organisational divisions. These structures demonstrated that 1) there is a tendency to view information security as a technical problem, and 2) to perceive information security as abstruse or removed from normal activities and processes. Here the employee is not an active enactor of information security, but one which follows the communicated direction provided by the IT department. In other words, the modalities of structure in Structures #2 and #3 reflect activities and processes which assume that information security is primarily enacted by the IT department, rather than by each employee.

The intention for using the theoretical framework based on structuration theory was for it to function as a problem-solving methodology. In the context of this study, the problem-solving is twofold: first as foremost, as explained above, it has identified factors which pose obstacles to the necessary ISMS integration. These are represented in Structure #2 and #3. The second manner it has contributed to a solution is by identifying opportunities for the ISMS to align with existing structures. Structure #4 represented a current structure at NorAg which facilitates an organisational-wide approach to organisational risk. NorAg has a tradition for managing considerable monetary values, while displaying proper governance and quality assurance to a range of stakeholders. This has created a deeply ingrained structure which provides modalities of structuration that guide employee activities and processes. This indicates that the upper management is accustomed to accounting for these risks in their decision-making processes and general management activities. Moreover, the employees are accustomed to adopting and integrating policies, regulations and guidelines into their everyday activities and organisational objectives. While the structure has traditionally been geared towards financial values, it is increasingly encompassing informational and technological values as well. Structure #5 does not identify a structure which is currently enacted, instead it identifies a budding desire for a new structure which can shape the organisational understanding and enactment of GDPR. This offers both a unique challenge and a unique opportunity. Because the structure, and the adherent modalities, do not exist, they would have to be created on a somewhat blank slate. This inevitably would introduce challenges in design and implementation. Yet, simultaneously, because there was a discernible desire for this structure to be introduced, it would allow for the careful crafting of a new and purposeful structure, which, presumably, would contain few legacies that would impact its function.

6. Limitations

This study has sought to hit a balance between theoretical significance and practical value, with the desire to seek somewhat novel discoveries. This is a fine line to walk, which opens for a variety of pitfalls. There are many aspects which can open the study up for criticism and it would be difficult to account for and respond to them all. However, through a focus on methodological and theoretical firmness, an effort has been made to allow for assessments, arguments and conclusions to be tried and tested. There are, however, particular limitations that must to be mentioned.

6.1 Implementation and/or Validation

Due to restrictions in time, the findings of the thesis have not yet been tested and implemented. It is therefore not possible to make any assertions about the validity of the findings and/or the utility value of the suggestions. However, as this process was initiated to complement the organisational changes in NorAg's ISMS, the thesis and the findings will be sent to NorAg to be read and assessed.

6.2 Structuration Theory

This study sought to have clear, practical implications. Yet, many of its dimensions remained largely theoretical. Structure #4 and #5 are identified as structures which can enable the integration of information security into existing structures. Yet, this study was unable to inquire into how this could occur. And this highlights a larger issue: it was never discussed exactly what initiates a process of structuration. The theoretical framework makes them appear somewhat distinct and purposeful designs which have been consciously created. Reality, one would assume, is that they are amalgamation of a range of factors, including internal and external forces, and unpredictable occurrences. The identification of structures might, hence, fail to provide decision-makers with any tangible understanding of how they ought to approach the challenges which are highlighted.

This leads to another, notable problem. The study revolved around analysing a highly empirical reality with a theoretical framework. The creator of said framework, Orlikowski, dubbed the framework a 'lens', indicating it is a way of perceiving the object of study. This is just one way of seeing the problem, and one can argue that this, inevitably, allows for the possibility of cherry-picking elements which fits into the theoretical framework, and disregarding those which don't. Furthermore, it exposes the study to the danger of creating theoretical abstractions which connection to empirical reality might be questionable, making the acceptance of the theoretical premise a necessity for the validity of the results. This was sought avoided through meticulous and careful explanation of both the research method and the problem-solving method.

6.3 No Methodological Guidance in the Assembly and Presentation of Structures

In total, five different structures were identified. Of these, Structure #1 can be claimed to be the most objective and the least open for subjective interpretation. This is because it directly reflects the position of NorAg's articulated ISMS. The identification and assembly of the Structures #2, #3, #4 and #5, however, were largely done based on the discretional abilities of the researcher. Frequently recurring postulations made by the interviewees were translated into representative modalities and these were then further assessed with the intention of placing them within a certain structure. It was the apparent interconnection and coherency between modalities which brought them together into a complete structure. Yet, the thesis did not offer a methodological explanation for how the modalities were identified from the management statements, nor how the modalities were combined. Moreover, the structures were not weighed. While there might be numerous structures within an organisation, there might be certain factors which makes some of them more important than others. Such a distinction has remained absent from this thesis. Including these aspects would, however, add an entirely new dimension to the thesis which would not be feasible to do justice in this text. Hence, this does instead open opportunities for further research and assessment.

6.4 The Problem-solving Methodology

Most of the interviewed upper management mentioned that they considered awareness and employee competence pivotal. Yet, it was merely a consideration which they were not familiar with how to achieve. Because of this, it proved difficult to encapsulate this sentiment into the problem-solving methodology. This indicates that the problem-solving methodology might not be sufficiently adequate at exploring less tangible inclinations and opportunities which have yet to directly manifest themselves into budding or functional structures. By not accounting for such inclinations, the wielder of this framework might run the risk of missing out on dynamics with untapped potential.

6.5 The Research Methodology

Action Theory was initially considered to be the most appropriate research methodology for the thesis. Two reasons in particular, however, led to the change to ADR. The first was the presence of an IT artefact, which made the ADR more apt. Secondly was the inability to engage in the cyclical iterations. In discussions with academic staff, it was advised that ADR would work better with the time limitations. As previously mentioned, the ADR proposed by Sein et al. (2011) did indeed not necessitate the cycles. However, the research project was not able to engage in the Building, Intervention, and Evaluation (BIE) step either. This was largely because the ISMS, as the IT artefact, had already been built. Instead, the focus has gone towards formalised learning. It can, hence, be argued that ADR is not optimal when there are time limitations or when the IT artefact is already built. Despite this, ADR is recognised as one of the best methodologies for researching IT artefacts when the researchers can take part in the project they study. This might, hence, suggest that there is potential need for the ADR to be developed for studies where it is not possible to engage in the BIE step. But inevitably,

In addition, the reliance on interviews of a limited number of managers can be considered a limitation due to two reasons in particular. Firstly, although the management represent their teams or divisions, there might be activities and processes which they are not aware of or having insight into. The management interviews might therefore only offer a reduced understanding of how information security is understood and enacted across the organisation. Secondly, the use of semi-structured interviews does not provide as tangible and quantifiable data points as certain other methodologies, such as for example a survey, would do. This reduces the recoverability of the research. However, methodologies such as survey limit the exploratory potential of the research, as surveys are more delimiting. If there had been more time, it could be beneficial to test the identified structures with more quantitative methodologies, such as a survey.

Lastly it must be mentioned that a larger sample size of case studies would be necessary to further test the validity of theoretical and practical contributions of the research.

6.6 People and Process, no Technology

The thesis followed a high-level trajectory and focused on the people and process dimensions of information security. The technological dimension was therefore largely omitted. This was deemed necessary due to limitations in scope and the high-level granularity of the study. But the theoretical results of the thesis might offer opportunities to inquire into how structuration influences the technological aspects of an ISMS.

6.7 Functional Structures, Functional Information Security

Identifying structural opportunities for information security through structuration theory assume that the existing structures are both functional and purposeful. If the problem-solving methodology identifies structures which are ineffective or undesirable, then it would presumably not be beneficial to attempt to integrate information security into these structures. Hence, the validity of the problem-solving methodology would also depend on the development of a methodology to determine the desirability of the identified structure. A future study might therefore want to develop such a methodology.

6.8 Systems Thinking

As has briefly been pointed out, a number of the concepts touched upon by structuration theory and Orlikowski's framework can also be found within systems theory and thinking. In systems thinking emphasis is put on understanding how single aspects of a system interconnect (Meadows 2008, p. 14), sharing many similarities to how this project has sought to understand how the interconnection in an organisation can affect the enactment of the ISMS. Systems theory and thinking could, therefore, potentially offer both increased conceptual solidity and added insights. The concept of resilience, for example, describe feedback loops which help a system maintain its elements and its function, as can be seen in Figures 5.1 and 5.2 (Meadows 2008, pp. 76-78). This could potentially offer tremendous insight into explaining why organisation struggle with changing existing structures.

Structure #1

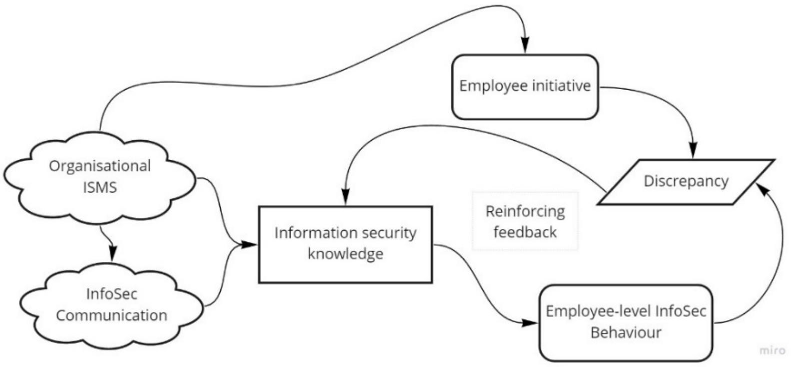


Figure 5.1 – Structure #1 in Systems Thinking

Structure #2 and #3

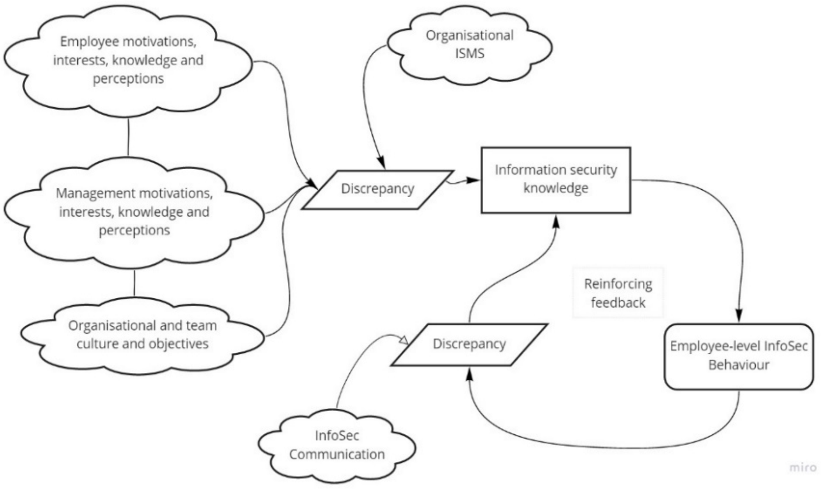

Employee motivations, interests, knowledge and perceptions
Organisational ISMS
Management motivations, interests, knowledge and perceptions
Discrepancy
Information security knowledge
Reinforcing feedback
Organisational and team culture and objectives
Discrepancy
Employee-level InfoSec Behaviour
InfoSec Communication
miro

Figure 5.2 – Structure #2 and #3 in Systems Thinking

However, systems theory and thinking has consciously not been fronted in this study. This has primarily been done because of limitations in space, and to ensure conceptual clarity. Due to the intricacy of structuration theory and Orlikowski’s lens, a decision was to avoid obfuscating the theoretical contributions with additional concepts, theories and methodologies.

7. Implications

With its twofold purpose of practical value and theoretical significance, the thesis has a number of implications. There are, however, three points which are of particular relevance to the topic and pursuit of this thesis:

1. When utilising an ISMS, it can be easy to assume that the information security enactment is a somewhat singular and clearly defined. Its properties and purposes are, after all, described in ISMSs such as ISO/IEC 27001, NIST CSF and NIST SP 800-53. Through the analysis enabled by the theoretical framework, however, it has been possible to discern that the social and organisational conditions might affect the integration of the ISMS. This has helped to exemplify that an organisation can have two (or more) understandings of how information security ought to work. On the one side, there can be a formal description of information security that exists in documents, communication and possibly be held by the IT department or information security team. While on the other, there can be a de facto information security, which are the prevailing perceptions and enactments that actually occur within and across the organisation. This de factor information security can potentially be separate from or contradictory to the formally recognised information security. This study, hence, demonstrates the need for organisations to analyse and understand to what extent the ISMS is functional and enacted within the organisational setting.

2. Moreover, the study demonstrates the multifaceted interconnectedness and intricacy of the relationship between information security and the organisation. Information security is widely recognised as an important challenge by most organisations. Yet, despite that there is political will to enact information security, many organisations fall short of cultivating the necessary resilience. This study has attempted to identify factors that might inhibit an organisation's ability to turn their political will into de facto increased resilience. As illustrated in this study, the alignment of information security requires organisational activities and processes to change, and/or the introduction of new activities and processes. Hence, this thesis has contributed to exemplifying why investing in technical controls and new technologies are not enough to achieve adequate information security resilience. This indicates that an organisation might have to engage in more structural changes to properly integrate information security and achieve

information security resilience.

3. For researchers, the utilisation of the theoretical framework offers an opportunity to better understand what influences employee enactment of information security (Orlikowski 2000, p. 423). Moreover, because this framework bridges concepts from literature on information security culture and alignment, it opens for new approaches and inquiries within these fields.

8. Conclusion

RQ #1 of this thesis was concerned identifying and understanding how the processes of structuration at NorAg affected the alignment of the ISMS across the organisation. The study has illustrated that ISMS alignment at NorAg will be affected by existing, reinforcing feedback loops. These feedback loops, identified as structures, contain norms and knowledge which leads to the recreation of certain activities and processes. While the official ISMS presumes that information security is actively enacted by each employee, two of the identified structures demonstrated that this is not the case. Information security is either considered to be the responsibility of the IT department, or it is perceived as difficult to enact because it is unclear how that should be done. Yet, two of the other identified structures provided opportunities for information security to align itself with existing (or nearly existing) activities and processes. This indicates that there an expectative misalignment between those responsible for the information security, represented by the IT department, and the wider organisation. This misalignment has led to confusion regarding how and by whom information security is enacted. While the findings can offer a multitude of insights, for the purpose of this case study the findings can be interpreted to suggest that the NorAg ISMS can particularly benefit from:

1) Shared, cross-organisational understanding of what purpose information security serves in the organisation;
2) Clear and distributed allocation of ISMS ownership and roles across the organisation;
3) Increased and aligned communication between IT and management; and
4) Comprehensive and tangible targets for how to enact the ISMS across the organisation.

RQ #2 was concerned with assessing the functionality of Orlikowski's theoretical framework to address the organisational problem. This theoretical framework provided a theoretical classification which allowed the identification of activities and processes which otherwise might have merely been deemed ‘normal’. As such, the theoretical framework opened for making connections which otherwise might not have been discernible. This provided a deeper insight into the recursive relationship between information security, as a structure, and the employee, as an agent. Thereby, the framework functioned as a problem-solving methodology which helped identify both 1) potential obstacles to ISMS integration and 2) potential opportunities for aligning the ISMS with organisational activities and processes.

9. References

AlHogail, A., 2015. “Design and validation of information security culture framework.” in Computers in Human Behavior, *49*, pp. 567-575.

AlHogail, A. and Mirza, A., 2014, January. “Information security culture: a definition and a literature review.” In 2014 World Congress on Computer Applications and Information Systems (WCCAIS) (pp. 1-7). IEEE.

Anderson, E.E., 2010. “Firm objectives, IT alignment, and information security.” in IBM Journal of Research and Development, 54(3), pp.5-1.

Association of Information Systems, 2011. ‘Senior Scholars' Basket of Journals.’ Accessed 20.07.20. https://aisnet.org/page/SeniorScholarBasket.

Avison, David, Richard Baskerville, and Michael D. Myers. 2007. "The structure of power in action research projects." In Information Systems Action Research, pp. 19-41. Springer, Boston, MA.

Baskerville, Richard L. 1999. "Investigating information systems with action research." Communications of the association for information systems, 2 (1): 19.

Baskerville, Richard, and A. Trevor Wood-Harper. 1998. "Diversity in information systems action research methods." In European Journal of information systems, 7 (2), pp. 90-107.

Bauer, Harald, Gundbert Scherf, Valerie von der Tann and Laura Klinkhammer. 2017. ‘Perspectives on transforming cybersecurity’ in Digital McKinsey and Global Risk Practice.

Bissell, Kelly, Ryan M. Lasalle and Paolo Dal Cin. 2020. ‘Lessons from leaders to master cybersecurity execution’ in Accenture. Accessed 19.07.20. https://www.accenture.com/no-en/insights/security/invest-cyber-resilience?src=LINKEDINJP.

Brotby, K., 2009. Information security governance: a practical development and implementation approach (Vol. 53). John Wiley & Sons.

Cisco Secure. 2020. ‘20 Cybersecurity Considerations for 2020.’ in The Cisco 2020 CISO Benchmark Report. Accessed 27.08.20. https://community.cisco.com/t5/security-blogs/20-cybersecurity-considerations-for-2020-download-the-cisco-2020/ba-p/4129788.

Chang, Shuchih Ernest, Shiou-Yu Chen, and Chun-Yen Chen. 2011. "Exploring the relationships between IT capabilities and information security management." in International Journal of Technology Management, 54, (2-3): 147-166.

Checkland, P. B. 1995. Soft systems methodology and its relevance to the development of information systems. In Stowell, F. A. (ed.), Information Systems Provision: The Contribution of Soft Systems Methodology, McGraw-Hill, Maidenhead, UK.

Checkland, Peter, and John Poulter. 2020. "Soft systems methodology." In Systems Approaches to Making Change: A Practical Guide, pp. 201-253. Springer, London.

Checkland, Peter., and Sue Holwell. 2006. "Action research: its nature and validity." In Information Systems Action Research: An Applied View of Emerging Concepts and Methods, edited by Checkland, Holwell and Kock: 3-18.

Coles-Kemp, L., 2009. Information security management: An entangled research challenge. Information security technical report, 14(4), pp.181-185.

Corriss, Laura. 2010. "Information security governance: Integrating security into the organizational culture." In Proceedings of the 2010 Workshop on Governance of Technology, Information and Policies, pp. 35-41.

Disterer, G. 2013. ‘ISO/IEC 27000, 27001 and 27002 for Information Security Management’. in Journal of Information Security, 4, pp. 92-100.

Farahmand, F., Atallah, M.J. and Spafford, E.H., 2012. Incentive alignment and risk perception: An information security application. IEEE Transactions on Engineering Management, 60 (2), pp. 238-246.

Fenz, S., Heurix, J., Neubauer, T. and Pechstein, F. 2014. "Current challenges in information security risk management", in Information Management & Computer Security, 22 (5), pp. 410-430.

e Figueiredo A.D., da Cunha P.R. 2007. Action Research and Design in Information Systems. In: Kock N. (eds) Information Systems Action Research. Integrated Series in Information Systems, vol 13. Springer, Boston, MA.

Fitzgerald, Todd. 2007. "Clarifying the roles of information security: 13 questions the CEO, CIO, and CISO must ask each other." In Information Systems Security, 16 (5): pp. 257-263.

Fredriksen, Eugene M. 2017. The CISO Journey: Life Lessons and Concepts to Accelerate Your Professional Development. CRC Press.

Giddens, Anthony. 1979. Central problems in social theory: Action, structure, and contradiction in social analysis. Univ of California Press.

Giddens, Anthony. 1984. The constitution of society: Outline of the theory of structuration. Univ of California Press.

Goodhue, D., and Straub, D. W. 1991. “Security Concerns of System Users: A Study of Perceptions of the Adequacy of Security Measures,” in Information and Management, 20 (1), pp. 13-27.

Hall, J.H., Sarkani, S. and Mazzuchi, T.A., 2011. “Impacts of organizational capabilities in information security.” in Information Management & Computer Security, 19 (3), pp. 155-176.

Herath, Tejaswini and H Raghav Rao. 2009. ‘Protection motivation and deterrence: a framework for security policy compliance in organisations.’ in European Journal of Information Systems, 18 (2), pp. 106-125.

Hevner, A. 2007. “A Three Cycle View of Design Science Research,” in Scandinavian Journal of Information Systems, 19 (2), Article 4.

Hevner, A. and Chatterjee, S., 2010. “Design science research in information systems.” In Design research in Information Systems, pp. 9-22. Springer, Boston, MA.

Hu, Qing, Tamara Dinev, Paul Hart, and Donna Cooke. 2012. "Managing employee compliance with information security policies: The critical role of top management and organizational culture." In Decision Sciences, 43 (4), pp. 615-660.

Hubbard, Douglas W., and Richard Seiersen. 2016. How to measure anything in cybersecurity risk. Hoboken: Wiley.

Humphreys, E., 2008. ‘Information security management standards: Compliance, governance and risk management’. in Information Security Technical Report, 13(4), pp.247-255.

IBM Security and Ponemon Institute. 2019. ‘2019 Cost of a Data Breach Report.’ Accessed 14.06.20. https://databreachcalculator.mybluemix.net/.

Ifinedo, P., 2012. ‘Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory.’ in Computers & Security, 31(1), pp. 83-95.

ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements

Jackson, G.W. and Rahman, S.S., 2017, December. Security Governance, Management and Strategic Alignment via Capabilities. In 2017 International Conference on Computational Science and Computational Intelligence (CSCI) (pp. 44-49). IEEE.

Johnston, A. C., & Hale, R. 2009. “Improved security through information security governance.” in Communications of the ACM, 52 (1), 126-129.

Jones, Matthew R., and Helena Karsten. 2008. "Giddens's structuration theory and information systems research." in MIS Quarterly 32 (1), pp. 127-157.

Karlsson, F., Åström, J. and Karlsson, M. (2015), "Information security culture – state-of-the-art review between 2000 and 2013," in Information and Computer Security, 23 (3), pp. 246-285.

Kayworth, Tim, and Dwayne Whitten. 2010. "Effective information security requires a balance of social and technology factors." In MIS Quarterly Executive, 9 (3), pp. 2012-52.

Knapp, K.J., Marshall, T.E., Kelly Rainer, R. and Nelson Ford, F. (2006), "Information security: management's effect on culture and policy," in Information Management & Computer Security, 14 (1), pp. 24-36.

KPMG. 2020. ‘All hands on deck: Key cyber security considerations for 2020’ in KPMG International Cooperative. Accessed 13.06.20. https://home.kpmg/xx/en/home/insights/2020/03/key-cyber-security-considerations-for-2020.html.

Lee A.S. (2007) Action is an Artifact. In: Kock N. (eds) Information Systems Action Research. Integrated Series in Information Systems, 13. Springer, Boston, MA

Levy, Heather Pemberton. 2015. “Lessons in How to Implement People-Centric Security” by Gartner. Accessed 03.09.20. https://www.gartner.com/smarterwithgartner/lessons-in-how-to-implement-people-centric-security/

Martins A., Elofe J. 2002. Information Security Culture. In: Ghonaimy M.A., El-Hadidi M.T., Aslan H.K. (eds) Security in the Information Society. IFIP Advances in Information and Communication Technology, vol 86. Springer, Boston, MA.

McKay, Judy, and Peter Marshall. 2007. "Driven by two masters, serving both." In Information Systems Action Research, pp. 131-158. Springer, Boston, MA.

Meadows, Donella H. 2008. Thinking In Systems a Primer, edited by Diana Wright. London ; Sterling, VA :Earthscan.

NIST, NIST Special Publication 800-53 (Rev. 4), 2013. Accessed: 04.06.20. https://web.nvd.nist.gov/view/800- 53/Rev4/home.

NIST CSF, NIST Cybersecurity Framework (version 1.1), 2018. Accessed: 04.06.20. https://www.nist.gov/cyberframework/framework.

Van Der Merwe, A. P. 2002. "Project management and business development: integrating strategy, structure, processes and projects." in International Journal of Project Management, 20 (5), pp. 401-411.

Van Niekerk, J. and Von Solms, R., 2006, July. “Understanding Information Security Culture: A Conceptual Framework.” In ISSA (pp. 1-10).

Van Niekerk, J.F. and Von Solms, R., 2010. “Information security culture: A management perspective.” in Computers & Security, 29 (4), pp. 476-486.

Van Niekerk, J.F. and R. Von Solms. 2010. “Information security culture: A management perspective.” In Computers & Security, 29 (4), pp. 476-486.

Jones, Matthew, Wanda Orlikowski, and Kamal Munir. 2004. "Structuration theory and information systems: A critical reappraisal." in Social Theory and Philosophy for Information Systems: 297-328.

Oates, Briony J. 2005. Researching information systems and computing. Sage.

Orlikowski, Wanda J. 2000. "Using technology and constituting structures: A practice lens for studying technology in organizations." in Organization Science, 11 (4), pp. 404-428.

Orlikowski, Wanda J., and Daniel Robey. 1991. "Information technology and the structuring of organizations." in Information Systems Research, 2 (2), pp. 143-169.

Orlikowski, Wanda J., and JoAnne Yates. 2006. "ICT and organizational change: a commentary." The Journal of Applied Behavioral Science, 42 (1), pp. 127-134.

Poole, Marshall Scott, and Gerardine DeSanctis. 2004. "Structuration theory in information systems research: Methods and controversies." In The Handbook of Information Systems Research, pp. 206-249. IGI Global.

Presthus, Wanda, and Bjørn Erik Munkvold. 2016. "How to frame your contribution to knowledge? A guide for junior researchers in information systems." In Norsk konferanse for organisasjoners bruk av IT, 24 (1).

Reece, R. P., and Bernd Carsten Stahl. 2015. "The professionalisation of information security: Perspectives of UK practitioners." in Computers & Security, 48, pp. 182-195.

Schein, E.H., 2010. Organizational culture and leadership (Vol. 2). John Wiley & Sons.

Sein, Maung K.; Henfridsson, Ola; Purao, Sandeep; Rossi, Matti; and Lindgren, Rikard. 2011. "Action Design Research," in MIS Quarterly, 35 (1), pp.37-56.

Von Solms, B., 2006. Information security–the fourth wave. Computers & security, 25(3), pp.165-168.

von Solms, B. 2006. “Information Security – The Fourth Wave.” In Computers & Security, 25 (3), pp. 165-168.

von Solms, R. and Van Niekerk, J., 2013. “From information security to cyber security.” In Computers & Security, 38, pp. 97-102.

Soomro, Z.A., Shah, M.H. and Ahmed, J., 2016. “Information security management needs more holistic approach: A literature review.” in International Journal of Information Management, 36 (2), pp. 215-225.

Stamp, M., 2011. Information security: principles and practice. John Wiley & Sons.

Straub, Detmar W., and Richard J. Welke. 1998. "Coping with systems risk: security planning models for management decision making." In MIS Quarterly, 22 (4), pp. 441-469.

Thomson, K.L., Von Solms, R. and Louw, L., 2006. “Cultivating an organizational information security culture.” In Computer Fraud & Security, (10), pp.7-11.

Tolbert, Pamela S., and Richard H. Hall. 2015. Organizations: Structures, processes and outcomes. Routledge.

Tweneboah-Kodua, S., Atsu, F. and Buchanan, W. (2018), "Impact of cyberattacks on stock performance: a comparative study", Information and Computer Security, 26 (5), pp. 637-652

Yayla, Ali Alper and Qing Hu. 2011. "The impact of information security events on the stock value of firms: The effect of contingency factors." Journal of Information Technology, 26 (1), pp. 60-77.

Valeriano, Brandon and Miguel Alberto Gomez. 2020. ‘The Failure of Academic Progress in Cybersecurity’ Council on Foreign Affairs, July, 2020. Accessed 02.08.20. https://www.cfr.org/blog/failure-academic-progress-cybersecurity.

Da Veiga, A. and Eloff, J.H., 2010. “A framework and assessment instrument for information security culture.” in Computers & Security, 29 (2), pp.196-207.

Da Veiga, A. and Martins, N., 2015. “Improving the information security culture through monitoring and implementation actions illustrated through a case study.” in Computers & Security, 49, pp.162-176.

Da Veiga, Adele, and Nico Martins. 2017. "Defining and identifying dominant information security cultures and subcultures." in Computers & Security, 70, pp. 72-94.

Vroom, C. and Von Solms, R., 2004. “Towards information security behavioural compliance.” in Computers & security, 23 (3), pp. 191-198.

Walsham G. and Han CK. 1991. “Structuration theory and information systems research.” in Journal of Applied Systems Analysis, 17, pp. 77–85.

Walsham, Geoff and Han, Chun-Kwong. 1990. "Structuration theory and information systems research". in ICIS 1990 Proceedings, 7, pp. 53-59.

Warkentin, M., and Johnston, A. C. 2008. “IT Governance and Organizational Design for Security Management,” in Information Security: Policies, Processes, and Practices, D. W. Straub, S. Goodman, and R. L. Baskerville (eds.), Armonk, NY: M. E. Sharpe, pp. 46-68.

West, Daune, and Mark H. Stansfield. 2001. "Structuring action and reflection in information systems action research studies using Checkland's FMA model." In Systemic Practice and Action Research, 14 (3), pp. 251-281.

Whitman, Michael E., and Herbert J. Mattord. 2011. Principles of information security. Cengage Learning.

Whittington, Richard. 2010. "Giddens, structuration theory and strategy as practice." Cambridge Handbook of Strategy as Practice: 109-126.

Willcocks, Leslie P., and John Mingers. 2004. Social theory and philosophy for information systems. John Wiley & Sons Ltd.

Appendix A

Kristiania University College

Ethical approval

Describe briefly the research aim and method(s) of your project: The research methodology is action design research. The research is conducted on the premises of the case study organisation. The data collection is done through document reviews and interviews. The purpose of the research is to elucidate the state of the ISMS alignment within the organisation.	
My research involves respondents/participants:	YES ■ NO □ (If yes, fill out consent form)
My research involves Personal data and/or Sensitive data: **Personal data include:** Name, Personal identification number, IP address **Sensitive data include:** Racial or ethnic background, Political, philosophical or religious opinion, Criminal record, Health related information, Sexual relations, Membership to trade unions.	YES ■ NO □ (If YES, fill out the Notification Form at Norsk samfunnsvitenskapelig datatjeneste (NSD, Personvernombudet for forskning – Data Protection Official for Research).
I have made a letter of consent	YES ■ N/A □
I have obtained permission from: Innovation Norway	YES ■ N/A □

Date and place	Student's signature	Supervisor's signature
23.05.2021	Henrik F Jenssen	Gebremariam Assres

AF/12.01.2021

Appendix B

Intervjuguide for masteroppgave

Semi-strukturert intervju

Enkeltpersoner

--

Spørsmål

Generelle

Kunne du beskrive din rolle i divisjonen?

Hva slags arbeidsoppgaver vil du generelt si at divisjonen din utfører?

- Hvilke teknologiske verktøy blir oftest anvendt for dette arbeidet?

Hvor involvert er du i risikoutredringer og beslutninger om informasjonssikkerhet?

- Eventuelt hvem i divisjonen er mest involvert i dette?

Divisjon

Hvilke teknologiske verktøy blir oftest brukt i divisjonen?

I hvilke aspekter opplever du at informasjonssikkerhet er mest relevant for din divisjon?

- Dette kan innebære alt fra aktiviteter til teknologier

Hvordan jobber du for å forankre informasjonssikkerhet i divisjonen?

- Er denne innsatsen koordinert med de andre lederne?

På hvilken måte støtter informasjonssikkerhet opp under aktivitene og målene til din divisjon?

- Er det aspekter ved informasjonssikkerhet som ikke støtter opp under aktivitene og målene?

Hvor risikoutsatt vil du si at din divisjon er?

- Med dette menes det både sannsynligheten for at dere skal ha en sikkerhetshendelse, og alvorsgraden ved en potensiell hendelse.

Organisasjon

Under hvilke omstendigheter mottar du oftest kommuniksjon om informasjonssikkerhet?

- Som et resultat av en hendelse? Ved innføringer av nye kontroller?
- Hvor kommer informasjonen fra? Ledergruppen? Fra IT?

Hvordan oppfatter du forholdet mellom organisasjonens strategi og objektiver, og informasjonssikkerhet?

- Er de sammhengende? Er de motstridende?

Hva er det du anser som den største utfordringen som påvirker organisasjonens informasjonssikkerhet?

Om informasjonssikkerheten burde endres, hvilke endringer ville bidratt til en mer effektiv informasjonssikkerhet?