

Exploring organisational elements of employee compliance behaviour

A human error perspective

CAMILLA WESSEL FRØHAUG
AMALIE WIDVEY

SUPERVISOR
Marko Ilmari Niemimaa

University of Agder, 2024
Faculty of Social Sciences
Department of Information Systems

Master

Acknowledgements

This study would not have been possible without the crucial feedback from our supervisor, Associate Professor Marko Ilmari Niemimaa at the Department of Information Systems at the University of Agder. Our meetings have been a vital part in keeping a steady and efficient pace in the process of finalising the thesis report, and we are forever grateful for the received guidance.

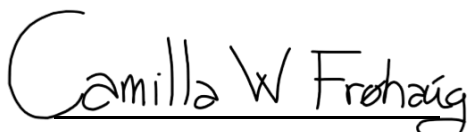
We would also like to give a special thanks to the anonymous interviewees who helped us gain insight and knowledge of the processes that comprise compliance behaviour at SWO. Their input and time has been extremely important to the project.

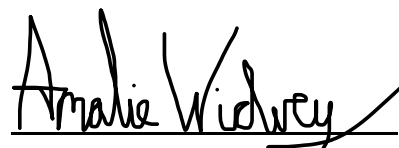
Further, we would like to thank our family, friends and loved ones who have cheered us on to the finish line. They have believed in us and been there since we started our studies - having their support has certainly helped to keep us motivated and confident in our work.

And finally, we would like to thank each other for motivation and encouragement along the way, as well as an honourable collaboration throughout the duration of our studies, and especially on our final project together - the master thesis.

Kristiansand,

June 3rd, 2023


Camilla Wessel Frøhaug


Amalie Widvey

Abstract

The aim of this master's thesis is to understand how organisational elements influence employees' compliance behaviour. To achieve this goal, we will examine the interviewees' responses to the challenges they experience with compliance and explore connections with the organisational conditions of the human error framework as well as a systematic literature review (SLR). By combining these insights, we will develop a holistic compliance behaviour framework. Our research question: *How do organisational elements impact employee compliance behaviours?*, will govern our exploration.

The primary purpose of the study is to investigate how organisational elements also influence compliance behaviour, as this is scarcely discussed in the literature. It is a well-known phenomenon that humans are seen as the weakest link, therefore we wanted to investigate the underlying organisational conditions that may have influenced this person's compliance behaviour.

In this thesis, we have conducted a qualitative case study where we have interviewed eight people related to a social welfare organisation (SWO) in Norway. The findings lead to the creation of a compliance behaviour framework consisting of five influential elements and how these altogether explain compliance behaviour, and the resulting consequences. By integrating our findings into the framework, it provides a visual understanding of how the organisation and the employees constitute compliance behaviour.

The findings showed that organisational elements such as culture, hierarchy, leadership, technology and structure influence employees' compliance behaviour in retrospect. We also discovered some new findings that impacted compliance, such as trust, environment and information sharing. Some of these areas had limited documentation, or were not previously documented. The findings are transferable to organisations outside the social welfare industry, and the research can thus be applied to a number of different sectors.

The implications for the research include a compliance behaviour framework, where we have findings on the same themes as in SLR, e.g. hierarchy, moral reasoning and technology, but that the perspective is different, where we see it through an organisational lens. In addition, we contribute by exploring new themes such as trust, environment and information sharing, and the change of perspective from individual to an organisational one. The practical implications from our research entails the identified stakeholders, the ability to implement our framework into consideration when creating policies and look for underlying root causes for compliance behaviour in an organisational context.

Table of contents

- 1. Introduction 7
 - 1.1 The purpose of the study and research question 8
 - 1.2 Research approach..... 8
 - 1.3 Thesis overview 8
- 2. Background 9
 - 2.1 Information security policies..... 9
 - 2.1.1 Compliance..... 11
 - 2.2 Individual compliance behaviour 11
 - 2.2.1 Human behaviour 12
 - 2.2.2 Peer behaviour 12
 - 2.2.3 Trust 13
 - 2.2.4 Moral reasoning..... 14
 - 2.2.5 Self-efficacy..... 15
 - 2.2.6 Workarounds 15
 - 2.2.7 Stress 16
 - 2.2.8 Time 17
 - 2.2.9 Punishments, rewards and costs..... 17
 - 2.2.10 Justifications 18
 - 2.3 Organisational aspects of compliance behaviour 18
 - 2.3.1 Designing ISP 19
 - 2.3.2 Information security culture 20
 - 2.3.3 Hierarchy 21
 - 2.3.4 Leadership..... 21
 - 2.3.5 Technology 22
 - 2.3.6 Monitoring..... 22
 - 2.4 Theoretical framework..... 23
 - 2.4.1 Human error framework..... 23
- 3. Research Approach 25
 - 3.1 Qualitative case study approach 25
 - 3.1.1 Research design..... 26
 - 3.2 Literature Review 27
 - 3.2.1 Method 27
 - 3.2.2 SLR criteria..... 27
 - 3.2.3 Search process..... 28
 - 3.2.4 Screening 29

3.2.5 Quality and eligibility assessment.....	29
3.2.6 Data processing and analysis.....	30
3.3 Data collection	33
3.3.1 The interview process.....	34
3.3.2 Interview limitations	35
3.4 Data analysis	36
3.5 Ethical considerations	37
4. Findings.....	38
4.1 Organisational structure	38
4.1.1 Environment	39
4.1.2 Information sharing.....	41
4.1.3 Technology	42
4.1.4 Top management	43
4.1.5 Security culture.....	44
4.1.6 Awareness.....	46
4.1.7 Outcomes of non-compliance	47
4.1.8 Trust	49
4.2 Organisational measures	50
4.2.1 Overall education.....	50
4.2.2 Access control	52
4.2.3 Monitoring.....	53
4.3 Work task	55
4.3.1 Time	56
4.3.2 Organisational origins of stress	57
5. Discussion	59
5.1 Compliance behaviour framework.....	59
5.2 Implications for research	60
5.2.1 The compliance behaviour framework.....	60
5.2.2 Our study's contributions	61
5.2.3 Perspective change	64
5.3 Practical implications.....	64
5.3.1 Navigating the change from individual to organisational.....	64
5.3.2 Policy design	65
5.4 Limitations.....	66
5.5 Future research.....	67
6. Conclusion.....	68
References	69

Appendix A: Interview guide	73
Appendix B: Consent form.....	76
Appendix C: Gantt chart	82

Figure list

Figure 1: Illustration of Kraemer & Carayon's framework on human error	24
Figure 2: Map of First-Generation Genres in Qualitative Research (edited) (Sarker et al., 2018).....	27
Figure 3: Systematic literature review stage overview	30
Figure 4: Nvivo categories from the analysis	37
Figure 5: Illustration of the compliance behaviour framework.....	60

Table list

Table 1: ISP definitions.....	10
Table 2: Illustrates the search words used to find the SLR literature.....	29
Table 3: Reclassification of research articles.....	33
Table 4: Interviewee information.....	34

1. Introduction

The prevailing discourse often portrays humans as the weakest link in information security management (ISM), emphasising the significance of individual compliance with security policies. However, such a narrative oversimplifies a complex landscape. While technical fortifications form a vital aspect of IS, the human element remains a critical yet often overlooked component. Despite advancements in technical controls, ensuring the integrity, availability, and confidentiality of information demands a comprehensive understanding of the interplay between organisational dynamics, individual behaviours, and technical measures (Williams et al., 2019; Altamimi et al., 2020).

Empirical evidence suggests that numerous organisational factors influence employee behaviours regarding IS policies (Hu et al., 2012; Williams et al., 2019; Herath & Rao, 2009). Only a limited amount of studies state various organisational reasons for human non-compliance behaviour, while countless others grasp around the human element as the sole contributor to non-compliance.

Investigating the impact of organisational elements on compliance behaviours is crucial in addressing the recurring issue of human error in security management (e.g. Khan & AlShare, 2019; Trang & Nastjuk, 2021; Koohang et al., 2020). While individuals are often considered as the weakest link in security policies (e.g. Myyry et al., 2009; Jiang, 2022), attributing non-compliance solely on individual shortcomings overlooks the broader systemic factors at play. An example could be explained with education: an individual shortcoming would be that the person does not see the value of security training, hence do not put in the work to learn it. While a systemic one, would be to have too little and not tailored training to the employees needs, not supporting them with sufficient knowledge and a good security culture, which may explain the individual shortcoming. Drawing inspiration from Carayon and Kraemer's (2007) human error framework, which highlights the role of latent organisational conditions in error occurrence, our research seeks to bridge the gap in existing literature by delving into the organisational elements influencing compliance behaviours.

In essence, by exploring the impact of organisational elements on employee compliance behaviours, we aim to contribute to a more holistic understanding of compliance dynamics within organisations. Compliance behaviours in this setting is defined as either being compliant, which means following information security policies (ISPs), or being non-compliant, meaning that the person is not following the ISPs and exhibiting unwanted behaviour. By uncovering the underlying organisational choices impacting compliance, we hope to pave the way for more effective strategies to enhance cybersecurity posture and mitigate risks associated with compliance behaviour.

1.1 The purpose of the study and research question

The purpose of this research is to explore if organisational aspects influence employees to ignore or adhere to policies, as well as understanding the broader scope to compliance through the framework of human error by Kraemer & Carayon (2007). To understand the problem area we will conduct an empirical study at a public sector organisation that deals with social welfare in Norway. The aim is to uncover details that influence employee compliance behaviour and identify the underlying organisational elements that contribute to it. This research strives to provide insights that can inform more effective IS strategies and interventions, without putting all the blame on the human element. By conducting a nuanced exploration of these elements, at a social welfare organisation (SWO), we seek to contribute to a deeper understanding of this problem area and pave the way for enhanced organisational security practices.

To conduct this research, we pose the question: *How do organisational elements impact employee compliance behaviours?*

1.2 Research approach

This study uses a qualitative research approach to explore the organisational elements that may influence employees compliance behaviour. The methods used to collect data for this study were semi-structured interviews. In addition to conducting a systematic literature review (SLR), to acquire an understanding of the current ISP field and to map out eventual shortcomings that our study could expand on, which in this case was the organisation's role in compliance behaviour.

1.3 Thesis overview

Chapter 1 - Introduction provides an overview of the problem, research question and explains the purpose of the study.

Chapter 2 - Background discusses the background information that forms the basis for this study.

Chapter 3 - Research approach justifies why the chosen research approach and design is suitable for this study, the process of the SLR, data collection and analysis, and limitations and ethical considerations we have encountered.

Chapter 4 - Findings presents the findings collected from the interviews.

Chapter 5 - Discussion discusses the findings from the interviews and SLR as well as the practical implications. We also present some directions for future research.

Chapter 6 - Conclusion provides a conclusion to the study and reflects on the limitations of the study.

2. Background

This chapter introduces an overview of the background work, and what current knowledge in these fields consists of. The background was a result of a literature review which is described in chapter 3.2. In the following subchapters, we will first elaborate on what ISP and compliance is, then explore the individual and organisational aspects that influence compliance behaviour, followed by a theoretical framework from which our research will draw inspiration from.

2.1 Information security policies

ISP constitutes a critical framework within different organisations, aimed at strengthening security, fortifying systems and preserving data integrity. Using the understanding that employee behaviours can pose significant challenges, ISPs encompass guidelines, rules, and procedures that are put together to foster compliance amongst employees (Kirlappos et al., 2013; Paananen et al., 2020).

Recent surveys have shown that insider threats are a significant concern for organisations, with 28% of data breaches involving insiders, and a staggering 90% of organisations reporting apprehensions about security risks from both malicious and non-malicious insiders (Luo et al., 2020). When employees fail to comply with organisational ISP requirements, information system vulnerability occurs, posing considerable risks to organisational resources, and despite efforts to bolster security measures, such breaches persist due to employees' non-compliance with ISP directives (Amankwa et al., 2018 & Koohang et al., 2019). Further, the financial impact of employee non-compliance is substantial, often resulting in losses amounting to millions of dollars (Herath & Rao, 2009).

Hedström et al. underscores the urgent need for organisations to address the problems with internal vulnerabilities, stating that "the majority of information security breaches are caused by incidents originating inside the organisation, where internal staff are identified as the most significant threat to information security" (Hedström et al., 2011, p.373). However, the diverse interpretations of ISPs among organisations highlight the necessity for tailored and comprehensive approaches to information security policy formulation and implementation, which might cause increased difficulty in creating an ISP that works for a particular organisation (Paananen et al., 2020). To enhance this further, definitions on ISP from several researchers are listed in table 1 below;

Definition	Author
<i>ISP is defined as a set of guidelines and procedures that organizations require employees to follow in order to ensure security activities and proper use of organizational information and technology assets</i>	(Shadbad & Biro, 2022, p.120)

<i>An ISP is often described as the declaration of a desired state of security and it employs words such as “security goals,” “strategy,” “objectives,” “intentions,” and “desirable achievements</i>	(Paananen et al., 2020, p.2)
<i>In other words, security policies and regulations are expressions of values, as well as sets of instructions</i>	(Hedström et al., 2011, p.373)
<i>In most behavioral ISS research, ISP reflects low-level policies which contains “normative lists of actions that the employees should (or should not) perform</i>	(Soliman & Mohammadnazar, 2022, p.6812)
<i>Policies are direction-setting documents for an organisation’s InfoSec that define roles and responsibilities, administrative and behavioural processes and procedures, as well as technologies, which constitute the key measures for promoting effective InfoSec management practices.</i>	(Niemimaa & Niemimaa, 2019, p.568)
<i>ISP assists users to effectively protect their systems. ISP refers to guidelines, requirements and rules that are set forward by management to target employees’ behaviors that enhance the organization’s information security</i>	(Koohang et al., 2020, p.231)
<i>Information security policy (ISP) is defined as the “state of roles and responsibilities of employees to safeguard the information and technology resources of their organization”</i>	(Khan & AlShare, 2019, p.7)

Table 1: ISP definitions

After understanding the different ways of expressing what an ISP is, we have concluded on the following definition:

“ISP is designed by the organisation to support employees in how to act to protect internal resources and systems. Ideally, it should help foster values and a desired security culture, preferably not conflict with work tasks, cover most of the processes in the organisation to eliminate workarounds, be achievable for employees to understand and execute, as well as tailored to the organisations needs.”

In the definitions above and the literature collected, the focus has been on the fact that the requirements in ISP are something employees must follow to ensure good security, and that non-compliance is a problem. The responsibility is usually directed at the employees, but there is little discussion of the role the organisation plays in this, and how ISP should be designed to secure the organisation without creating conflicts with work tasks and internal processes that the employees ultimately have to deal with.

2.1.1 Compliance

ISP compliance is a critical aspect of organisational security efforts, requiring employees to follow the standards, guidelines, and practices outlined in ISPs to safeguard information and technology resources (Nord et al., 2022; Hwang et al., 2017; Amankwa et al., 2022). Note that "compliance" can be an ambiguous term that can refer 1) to the organisational level 2) to the individual level. The difference is that organisational compliance refers to how an organisation meets a criterion, while ISP compliance refers to how an individual follows an ISP (Niemimaa, 2023). When we refer to organisational compliance, we are talking about elements within the organisation that affect individual compliance.

Further, the important role of employee awareness in complying with ISP is underscored, emphasising the need for individuals to understand and internalise the purpose and requirements of these policies (Nord et al., 2022; Koohang et al., 2020). Compliance intention, defined as the willingness to execute ISP requirements, reflects employees' commitment to protecting organisational assets from potential security breaches (Koohang et al., 2020; Koohang et al., 2019). Furthermore, employee compliance can be motivated by various aspects, including the desire to avoid punishment or receive rewards, adherence to societal norms, or an understanding of the rationale behind ISP rules (Khatib & Barki, 2022).

Rogier Woltjer describes a need for a focus on vocabulary for compliance and violations of IS policies, which might help bridge the gap to employee awareness (Woltjer, 2017). At its core, ISP compliance entails individuals carrying out essential security activities to uphold IS as defined by organisational policies (Altamimi et al., 2020). Overall, fostering a culture of awareness and commitment to ISP among employees is essential for mitigating security risks and ensuring the integrity and confidentiality of organisational information (Nord et al., 2022; Hwang et al., 2017; Amankwa et al., 2022).

2.2 Individual compliance behaviour

More than 90% of all organisations encounter at least one data security issue a year, and most of them occur due to employee non-compliance (Khan & AISHare, 2019). Internal security threat exists when employees fail to comply with the ISP, whether intentionally or unintentionally (Aggarwal & Dhurkari, 2023; Altamimi et al., 2020; Trang & Nastjuk, 2021; Koohang et al., 2020). A lack of compliance can lead to a system or device being vulnerable to security risks and threats (Koohang et al., 2020). Understanding the resource vulnerability protects the organisation's assets from security threats, and because of these risks, it is vital for the organisation that employees comply with the ISP (Koohang et al., 2020). To better understand what plays into employee non-compliance, this chapter will elaborate on the various aspects that influence employees behaviour.

2.2.1 Human behaviour

Human behaviour is a complex interplay of beliefs, motivations, and evaluations (Williams et al., 2019). Attitudes toward actions are shaped by behavioural beliefs, normative beliefs, and control beliefs, which collectively influence behavioural intentions and actions (Williams et al., 2019). Extrinsic motivation, driven by external rewards or punishments, and intrinsic motivation, derived from internal satisfaction, both play significant roles in influencing behaviour (Chen & Tyran, 2023). While extrinsic motivation may involve factors like monetary rewards or public praise, intrinsic motivation arises from internal satisfaction and enjoyment (Chen & Tyran, 2023).

Evaluation of one's actions against defined standards is integral to human behaviour, and when individuals anticipate evaluation, they tend to exhibit desirable behaviours and avoid undesirable ones (Amankwa et al., 2021). Moreover, distinctions exist between malicious and non-malicious violations of ISPs - non-malicious violations occur unintentionally, without the intent to harm IT assets (Altamimi et al., 2020).

In the area of IS, the value-based compliance model provides insights into human behaviour (Hedström et al., 2011). To further explain what is involved in a value conflict with ISP, Hedström developed a new term, information security action (ISA), to explain the differences between desired actions in the organisation, known as described ISAs, and performed actions, known as actual ISAs. While this may seem like a new term, it is merely an explanation of ISP and compliance. Prescribed ISAs represent ideal regulations, akin to an organisation's explanation or justification of a given pattern of activity. Actual ISAs, however, reflect the actions performed in daily practice, influenced by the actor's goals and values. During their data collection, Hedström et al. focused on comparing prescribed ISAs with actual ISAs to identify value conflicts and underlying rationalities (Hedström et al., 2011). The comparison between the two helps in understanding discrepancies between intended and actual behaviour. The situational nature of human behaviour means that action strategies and goals adapt to the current context, with values guiding decision-making during value conflicts (Hedström et al., 2011). The value conflicts in this context, it is a conflict between complying or breaking with ISP.

2.2.2 Peer behaviour

Employees often take actions based on the behaviour of their peers, and they rely heavily on each other to overcome daily practices issues, especially issues related to security controls (Herath and Rao, 2009; Altamimi et al., 2020). Employees' non-compliance is therefore often motivated by the behaviour of their colleagues (Herath and Rao, 2009; Hwang et al., 2017; Hu et al., 2012; Williams et al., 2019; Altamimi et al., 2020). This means that if employees perceive that colleagues are not following the security policy, they may think that it is sensible not to comply either (Hwang et al., 2017).

Hu et al. states that “intention is assumed to capture the motivational factors that influence an individual’s behaviour” (Hu et al., 2012, p.623). This can be understood through the Theory of Planned Behaviour (TPB) framework, where human behaviour is driven by three factors: attitude towards the behaviour (ATT), subjective norm (SN) and perceived behavioural control (PBC) (Hu et al., 2012; Williams et al., 2019). ATT refers to a person's assessment of a behaviour of interest. SN reflects the person's perception of whether the behaviour is accepted by the social circle in which the person is located. In an organisational context, the person's social circle consists of colleagues, subordinates and superiors. PBC is the experienced ease or difficulty of performing a behaviour and self-efficacy to perform it (Hu et al., 2012).

One study shows that individuals create their own personal behaviour based on interactions with colleagues, leading them to follow the ISP as they see fit (Williams et al., 2019). In addition, the social impact of peer behaviour influences individuals to follow and imitate each other's actions and ultimately use the same justifications for not complying with ISP (Altamimi et al., 2020; Herath & Rao, 2009). Employees' perception that others comply with the security policies also proved to be an important factor for employees' intention to comply with the policies themselves (Herath & Rao, 2009). In other words, the peer behaviour and culture in the organisation can influence employees to either comply with or violate the security policy.

2.2.3 Trust

Trust is multifaceted, encompassing a willingness to rely on others while being vulnerable to their actions (Doney et al., 1998; Koohang et al., 2019). It is rooted in shared social expectations within environments, where trust creates mutual expectations upheld by all involved parties (Koohang et al., 2019). Moreover, trust involves an individual's belief in others' ethical behaviour under various influences, such as subjective norms and confidence (Chang et al., 2015). As emphasised by Doney et al. (1998), trust involves a fundamental condition where one must be vulnerable to the other party, highlighting its intrinsic nature within human interactions.

Studies highlight three key components of trust: competence, benevolence, and integrity (Koohang et al., 2020). Competence trust revolves around the trustee's ability to fulfil their responsibilities, benevolence trust concerns their goodwill and care for others, and integrity trust focuses on upholding acceptable principles and standards (Koohang et al., 2020). Trust plays a crucial role in various forms of exchange, reducing transaction costs in uncertain environments and contributing to effective implementation of strategies within organisations (Doney et al., 1998). Furthermore, trust fosters effective leadership, motivating individuals to assume greater responsibilities (Paliszkievicz, 2019).

Within organisations, trust is an expectation that positive outcomes will result from their actions (Paliszkievicz, 2019). Trust influences compliance with ISPs - trust in policies and colleagues positively affect employee commitment, work attitudes, performance

and compliance (Chang et al., 2015; Li et al., 2020). Conversely, distrust may lead to reluctance to cooperate, potentially hindering organisational goals. Spying on employees and the implementations of such systems is by Chang et al. described as a way of manipulating a computing base, and can cause serious damage to the trust relationship between employees and the organisation (Chang et al., 2015). Lack of trust in monitoring measures can lead to reluctance and non-compliance among employees (Chang et al., 2015).

Policies favouring compliance and employee awareness of security risks can reduce reliance on expensive security mechanisms. Trust in the organisation induces compliance, while clever monitoring that can detect violators makes employees more conscious and less likely to abuse trust intentionally (Kirlappos et al., 2013). In line with this, Khan & AlShare (2019) caution that trust, while essential for productivity, can also prompt risky behaviours such as password sharing among colleagues, exposing organisations to significant security risks (Khan & AlShare, 2019).

Interestingly, Norway stands out as a country with one of the highest levels of trust in the population, with Norwegians showing increasing levels of trust over the past 20 years (Barstad & Sandvik, 2015). This cultural context underscores the importance of trust in shaping societal dynamics and organisational behaviour. Trust not only facilitates cooperation and collaboration but also influences individual attitudes and decision-making processes within organisations.

2.2.4 Moral reasoning

In understanding employees' adherence to ISPs, it becomes evident that moral reasoning plays a role (Nord et al., 2022). Compliance with common ISP violations, such as password sharing, personal internet use at work, and selling confidential data, is influenced by work context, personal moral beliefs, and the perceived likelihood of detection (Nord et al., 2022). It is further emphasised that employees' perception of the harmfulness of deviant actions are decisive for their moral assessment of how serious such violations are. This perception of harmfulness is shaped by situational cues, such as the type of assets involved and the intent behind the deviant act (Luo et al., 2020).

Additionally, Myyry et al. (2009) emphasise the relevance of moral reasoning in the context of ISPs, positing that decisions to violate such policies can be understood as moral conflicts. These conflicts arise when individuals feel compelled to prioritise completion of moral obligations, such as assisting others versus adhering to security protocols, as exemplified by the violation of tailgating (Myyry et al., 2009). In addition to just conflicts, another part of understanding human behaviour and moral reasoning is an individual's values. Research in moral psychology, particularly highlighted by Myyry et al. (2009), suggests that individual values play a pivotal role in shaping behaviour and attitudes. In situations where individuals face temptations to violate norms, such as non-compliance with IS policies, values like self-discipline become crucial. Myyry et al. further highlight that individuals who perceive punishment or risk

with non-compliance, are more likely to obey IS policies. Understanding the relationship between normative beliefs, values, and IS behaviour is essential for designing effective security measures within organisations.

2.2.5 Self-efficacy

The self-efficacy (SE) theory was introduced by Bandura. The theory is based on the idea that one must be motivated to complete a given task or perform an action that is dependent on competence (Williams et al., 2019; Koohang et al., 2020). It is also about the individual's perception of their own abilities to achieve a particular goal, which in this case is the organisation's ISP. SE in this context refers to the individual's perception of how simple, straightforward and effortless it is to protect information systems from security threats (Koohang et al., 2020).

Employees with low SE in terms of security knowledge or negative attitudes towards security may give up or fail to act because they assume that their behaviour will have no impact (Nord et al., 2022). Studies across the field agree that SE has a positive impact on users' behaviour when it comes to complying with ISP (Koohang et al., 2020). Williams et al. believe that SE is the most important prerequisite for achieving behavioural change in security, where leaders play an important role and should set a good example for employees to imitate, thereby contributing to increased self-efficacy (Williams et al., 2019).

2.2.6 Workarounds

A workaround is a targeted adaptation, improvisation or other change to an existing system to overcome, bypass or reduce the impact of obstacles, gaps, management expectations or structural limitations. These are perceived to hinder the participants from achieving a desired level of productivity as well as organisational and/or personal goals (Woltjer, 2017). Employees perceive that IS policies are counterproductive because they prevent them from performing their daily tasks effectively (Williams et al., 2019; Li et al., 2020; Bulgurcu et al., 2010; Herath & Rao, 2009). Employees may therefore violate ISPs if they consider the policies to be a threat to their freedom, an impediment to work and an invasion of privacy (Li et al., 2020; Nord et al., 2022). Workarounds are partially different from ISP compliance, where workarounds-as-improvisations are used more regularly by employees who perceive more conflicts between IS and other goals, and employees who have more IS knowledge (Woltjer, 2017). He further states that workarounds-as-non-compliance or trade-offs are experienced more by employees in organisations that handle information with high security requirements and by individuals who perform tasks with high IS requirements.

Workarounds can be categorised into two forms by Woltjer: improvisation and compliance;

- (1) Workarounds as actions performed when the IS policy does not specify what is to be done, here called workaround-as-improvisation.

(2) Workarounds as actions that are performed due to perceived benefits in favour of other work goals, such as efficiency, integrity or quality of work, and which are not considered to be in compliance with the IS policy, referred to as workarounds-as-non-compliance.

In regards to IS in organisations, the responsibility of whether to follow the organisation's ISP or ignore it is assigned to employees (Herath & Rao, 2009). Organisations often set high targets for productivity and security but fail to manage the inherent workarounds and trade-offs, leading employees to prioritise productivity over security due to both task focus and personal benefit maximisation (Kirlappos et al., 2013). According to Woltjer, the more challenging the work is from an IS perspective, the more probable it is that the IS goal will conflict with other work goals (Woltjer, 2017). Simultaneously, most employees focus is not on security, but on performing their primary tasks efficiently (Kirlappos et al., 2013). This means that employees are willing to spend limited time and effort on secondary tasks such as security. Sometimes even meeting the security requirements can conflict with employees' primary tasks, forcing them to sacrifice IS to fulfil their primary tasks (Bulgurcu et al., 2010).

2.2.7 Stress

Research has consistently highlighted the critical role of stress in shaping compliance behaviours regarding ISP regulations (Trang & Nastjuk, 2021; Aggarwal & Dhurkari, 2023). Participants subjected to high-stress conditions exhibit notably higher levels of non-compliance behaviours, indicating a direct link between stress and deviation from established ISP guidelines (Trang & Nastjuk, 2021). This stress stems from various sources, including work overload, complexity, uncertainty of security requirements, and technology-related stressors (Li et al., 2020; Aggarwal & Dhurkari, 2023). Moreover, stress induced by time constraints further provokes non-compliance behaviour in the workplace, illustrating the detrimental impact of stressors on adherence to ISP protocols (Trang & Nastjuk, 2021).

It is important to mention that stress is to be regarded as a multifaceted phenomenon that will limit the potential conceptual clarity, and is therefore difficult to have a single definition that covers all areas of stress. There are some scholars who refer to stress as a stimulus, while others might refer to it as a response (Aggarwal & Dhurkari, 2023). The complexity and inconvenience of ISP regulations themselves contribute to stress among employees, leading to non-compliance as individuals perceive the requirements as unnecessary and laborious (Aggarwal & Dhurkari, 2023).

Technostress, characterised by feelings of not being able to handle IT demands, is a significant contributor to ISP non-compliance (Shadbad & Biro, 2022). High levels of technostress lead users to rationalise violations of ISP regulations, driven by a perceived inability to effectively manage IT-related tasks. The authors further state that stress arises from various technostress creators, including workload, uncertainty, and

insecurity associated with IT use, further reinforcing the link between stress and non-compliance behaviours.

2.2.8 Time

Hedström et al. found that many value conflicts are linked to time pressure, as IS routines are perceived as burdensome (Hedström et al., 2011). In a situation with limited time available, the individual's priority is to reduce the amount of information being processed, for example by filtering out the most critical information or neglecting certain information (Trang & Nastjuk, 2021). Li et al. argue that security policies are stressful for employees as they often have to invest extra time and resources to comply with security requirements (Li et al., 2020). Time pressure can cause employees to prioritise completing tasks, while secondary tasks such as security are neglected and lead to non-compliance with ISPs (Trang & Nastjuk, 2021). An example of this could be Hedström et al.'s findings that healthcare professionals develop routines to support an effective and 'easy' way of working due to time constraints. However, these routines often conflicted with the IS values of confidentiality and accountability (Hedström et al., 2011). The trade-offs in this conflict leads to more effective work for the employees, but loss of security for the organisation.

2.2.9 Punishments, rewards and costs

The efficacy of punishment, rewards, and costs in shaping employee compliance is a subject of ongoing debate. Herath and Rao (2009) contend that while the literature generally suggests a negative correlation between the severity of punishment and deviant behaviour, actual organisational sanctions may not significantly influence employee compliance. They further state that this may stem from employees perceiving termination for security breaches as isolated incidents rather than systemic issues. Similarly, Williams et al. (2019) found that sanctions or penalties have no discernible impact on compliance with ISPs. Contrary to popular belief, some argue that fear-based sanctions in security policies might not stop employees from ignoring rules when facing security threats (Li et al., 2020).

The intention to comply with ISPs is more influenced by intrinsic factors such as role values, fear, and habit rather than external motivators like punishments or rewards (Aggarwal & Dhurkari, 2023). Moreover, research posits that compliance is not significantly impacted by punishments, rewards, or complementary conditions, but rather by individual perceptions of role values and habitual behaviours (Aggarwal & Dhurkari, 2023). This aligns with the notion that employees may continue to behave insecurely despite being fully aware of the potential consequences (Aggarwal & Dhurkari, 2023).

Khatib and Barki (2022) expand on rational choice theory, suggesting that employees weigh the costs and rewards of compliant and non-compliant behaviours when deciding their course of action. They argue that when the costs of non-compliance are

low and the rewards are high, individuals are more likely to engage in non-compliant behaviour. Conversely, when both costs and rewards are high, employees are more inclined to comply with organisational policies (Khatib & Barki, 2022). Additionally, situational factors play a role in the deterrence effect of formal sanctions; for instance, while sanction severity may deter serious violations, it may not effectively deter less severe infractions like password sharing (Luo et al., 2020).

2.2.10 Justifications

According to Bulgurcu et al. (2010), employees' attitudes toward compliance behaviour are shaped by their beliefs regarding the consequences, weighing the costs and benefits involved. This rationalisation process often leads individuals to employ neutralisation techniques, rendering behavioural norms inoperative and alleviating feelings of shame or guilt (Altamimi et al., 2020; Shadbad & Biros, 2022).

Kirlappos et al. (2013) found that employees sometimes share passwords to expedite work processes or assist colleagues, justifying their actions by the necessity of task completion. Soliman & Mohammadnazar (2022) argue that overlooking the contextual factors surrounding ISP violations may lead to unjustified punitive measures, emphasising the importance of understanding the rationale behind non-compliance.

Moreover, descriptive norms, reflecting what others do, often override injunctive norms prescribed by ISPs, further influencing employees' behaviours (Altamimi et al., 2020). Luo et al. (2020) contend that rule-breaking behaviours are situational, dependent on both individual morality and contextual triggers. Therefore, the justification for violating ISPs varies based on the specific features of the setting and the moral interpretation of the individual (Soliman & Mohammadnazar, 2022; Shadbad & Biros, 2022; Luo et al., 2020).

2.3 Organisational aspects of compliance behaviour

Studies show there is a lot of research on why individuals follow or break IS rules, but there's not much on how organisational factors affect employee behaviour in this area. Most organisations seem to be unaware of or choose to overlook the impact of security mechanisms on their employees. Studies show that in the workplace context, organisations assume that employees can easily cope with the effort involved in complying with security requirements, and that in spite of organisational influential initiatives, employee ISP non-compliance continue to be a threat to IS (Kirlappos et al., 2013; Li et al., 2020). Williams et al. (2019) emphasise that one of the reasons for non-compliance is that it is not clear to employees and management who is responsible for information security. In certain situations, employees' own rules may be more tailored to the specific situation than what is stated in the policy. In such cases, a dilemma arises that has not been widely addressed previously by information security system researchers, regarding what needs to be corrected, the employee's behaviour or the policy (Soliman & Mohammadnazar, 2022).

2.3.1 Designing ISP

Designing and implementing effective ISPs is an important part in mitigating IS threats within organisations. Trang & Nastjuk (2021) emphasises the significance of ISPs in regulating employee security behaviour, underscoring the importance of employee training in reducing security threats. It is also pointed out that a crucial gap in understanding the drivers of security behaviour lies beyond the interface, suggesting that policies should be re-designed to align with human capabilities and real security needs, rather than solely relying on expert opinion (Kirlappos et al., 2013). While organisations establish ISPs to give employees guidelines for ensuring IS during job tasks, mere policy creation is insufficient to ensure compliance (Bulgurcu et al., 2010). Hu et al. (2012) argue that effective security policies must be integrated into organisational culture to be truly impactful. Some employees might find themselves disconnected from the policy design process, as policies are typically crafted to align with the perceptions and expectations of policymakers regarding employee behaviour (Kirlappos et al., 2013). Consequently, employees often lack meaningful insights or contributions to the development of these policies. Organisations should include employees' sanction expectations when it comes to different situations, so that the employees have a clear view of what might end up being a consequence for a specific action (Luo et al., 2020).

Moreover, the formulation of policies tends to rely heavily on past failures rather than scientific principles (Kirlappos et al., 2013). This approach may limit the effectiveness and adaptability of policies, potentially hindering their ability to address emerging challenges or evolving organisational needs. It is important to create policies that resonate with employees and address their actual security concerns. Additionally, there should be a strong integration of scientific principles to ensure policies are evidence-based and responsive to the dynamic nature of workplace environments (Trang & Nastjuk, 2021; Kirlappos et al., 2013). To include or engage the employees in the ISP design process can have a positive lingering effect on the organisation as a whole. Building trust and enhancing collaboration builds social capital and provides incentives for compliance and mutual beliefs, which in turn can enhance the level of security protection (Koohang et al., 2019).

Kirlappos et al. (2013) describes an integrated approach to ISP development, suggesting that combining ISP lifecycle with existing processes, such as general management and strategic processes, can enhance their effectiveness. These aspects enhance the need to tailor ISPs to the specific characteristics and environments of organisations, rather than adopting a one-size-fits-all approach, as the working climates are vastly different between organisations (Kirlappos et al., 2013; Soliman & Mohammadnazar, 2022). By integrating ISPs into existing processes and considering organisational context, organisations can develop policies that are not only effective but also practical and feasible for implementation (Paananen et al., 2020; Soliman & Mohammadnazar, 2022). This not only facilitates user compliance but also enhances the IS management's understanding of users' values, thereby enabling the design of

policies aligned with users' rationality (Paananen et al., 2020; Hedström et al., 2011). By considering these insights and tailoring ISPs to organisational context and user values, organisations can develop more effective policies that not only mitigate security risks but also promote user adherence and support organisational goals.

2.3.2 Information security culture

Information security culture (ISC) plays a pivotal role in safeguarding information assets and guiding employees' behaviours towards compliance with ISP (Nasir et al., 2022; Amankwa et al., 2021). It encompasses attitudes, assumptions, beliefs, values, and knowledge that employees employ when interacting with organisational systems and procedures, and such a culture is cultivated through the establishment of policies, standards, training, and educational programs within the organisation (Khan & AlShare, 2019; Amankwa et al., 2021). An effective ISC is vital in mitigating the limitations of technological controls within organisations (Nasir et al., 2022). Organisational culture, being a significant determinant of ISC, influences employees' compliance with ISP (Amankwa et al., 2022).

The distinction between IT and non-IT professionals within organisations is not only crucial but also intricate, as it significantly impacts their perceptions and compliance with IS measures (Nasir et al., 2022). Non-IT professionals, often lacking in-depth knowledge and awareness of IT systems and security protocols, tend to rely more heavily on organisational culture and engagement to guide their behaviours towards IS (Nasir et al., 2022). Conversely, IT professionals with technical expertise, may have a more nuanced understanding of security measures but can still be influenced by organisational culture when it comes to compliance. Effectively managing organisational culture is important, as it can either bolster or undermine IS objectives (Karlsson et al., 2022; Chang et al., 2015). Hu et al. (2012) describes that organisational culture shapes and guides how employees behave, based on the employees' shared values, the commitment to the organisation, and how the leadership is influential in this movement.

To foster a shared belief in IS across all employee groups, Koohang et al. (2020) explains that organisations must invest in areas of comprehensive education and awareness. By providing training programs, resources, and regular communication about the importance of IS, organisations can create a sense of responsibility and ownership among employees, regardless of their technical background.

The creation of ISP compliance culture is essential in promoting adherence to ISP among employees at all organisational levels (Amankwa et al., 2020). Amankwa et al. (2018) explains that organisational culture emerges as a crucial factor of ISC in existing literature. Understanding the influence of organisational culture on IS grants a well-reasoned background for exploring the organisational context and how implementation of security measures has an impact.

2.3.3 Hierarchy

Different studies in the ISP context mentions top management as an influential aspect on employees' intention to comply (Hu et al., 2012; Hwang et al., 2017; Kirlappos et al., 2013). Some studies show that the participation of upper management has a direct influence on employees' compliance behaviour, while others argue that top management's involvement has low significant impact, because top management is more distant from day-to-day operations (Hu et al., 2012). The low significance can be explained by the relative hierarchical distance between top management and employees, and the fact that top management's influence on employee attitudes is mediated by the organisational culture (Hu et al., 2012). Within this context, hierarchy, often associated with bureaucratic or control-oriented cultures, is a significant aspect. Research by Hedström et al. (2011) indicates that organisations with hierarchical cultures tend to prioritise IS management principles, with employees exhibiting greater compliance with ISPs.

A further challenge with the involvement of top management addressed by Kirlappos et al., is that compliance enforcement creates tension and reinforces the value gap between those who enforce (top management) the security rules and the rest of the organisation (the employees). Employee's frustration with security is directed back to the enforcers, potentially causing any information from them to be treated with scepticism or ignored altogether (Kirlappos et al., 2013). The authors further explain that this creates a general negative attitude towards IS, which can discourage compliance with security mechanisms - even when they are sensible and well designed. In contrast, managing the employees to follow the ISP is the most challenging aspect of IT security (Hwang et al., 2017).

2.3.4 Leadership

Management plays a vital role when it comes to IS, and management has to assume responsibility for the management of IS in organisations (Koohang et al., 2020; Herath & Rao, 2009; Khan & AlShare, 2019). The authors further state IS is a top management issue, and the commitment and effective leadership assist the implementation and enforcement of ISP in organisations (Koohang et al., 2020). IS is not just a technical issue - leadership plays an essential part in providing a work environment that supports the organisation's security culture (Khan & AlShare, 2019). Hu et al. (2012) also discuss how top management's participation in IS initiatives has both direct and indirect impacts on employees' attitudes towards, subjective norm for, and perceived control over ISP compliance.

However, management influence can go both ways. In the most severe cases, such as abuse of supervision or safety fatigue and frustration, it can lead to employees reducing their overall willingness to comply with requirements and their organisational commitment (Nord et al., 2022). According to Kirlappos et al. (2013), enforced compliance with time-consuming mechanisms divert valuable employee resources and reduce organisational productivity. Surprisingly, large parts of the organisation (e.g.

line managers) are complicit in employees not following the policy because they value productivity more, despite what the policy dictates. Research found that one of the main causes of employee's non-adherence to the policies were due to the CEO being perceived as passive when it came to promoting and complying with the established ISPs (Hu et al., 2012). The authors further discuss that after the CEO changed the attitude towards IS and actively engaged in IS issues, there were significant changes in employees' attitudes towards compliance with ISP.

2.3.5 Technology

In numerous instances, employees have demonstrated an acute awareness of the heightened risks associated with their actions, often blaming their non-compliance on shortcomings in the organisation's technology infrastructure (Kirlappos et al., 2013). Despite this awareness, employees frequently resort to circumventing security measures to maintain operational continuity, perceiving organisational priorities as favouring productivity over strict security protocols. This harmonious relationship between employees and organisational technology underscores the critical role of technological solutions in cybersecurity contexts. Research highlights the role of robust security systems, comprehensive education, and enhanced visibility in reducing instances of non-compliance among employees (Hwang et al., 2017).

2.3.6 Monitoring

In the IS context, it is possible to enforce sanctions if the organisation is able to detect employee misbehaviour (Herath & Rao, 2009). The authors further discuss how researchers have emphasised the relevance of auditing mechanisms to inspect the security behaviour of end users. The purpose of implementing employee monitoring is to increase employee productivity and performance at work, and it is therefore essential to understand how employee monitoring affects the commitment to the organisation (Chang et al., 2015). It can also be difficult to monitor employee actions related to ISP compliance (Herath & Rao, 2009; Williams et al., 2019; Kirlappos et al., 2013). For example, network monitoring can be used to track online behaviour or install cameras to achieve a certain level of security, but behaviours such as writing down or sharing passwords with peers cannot be monitored (Herath & Rao, 2009). Employee monitoring can be designed in different ways to control access and keep track of records, and policies are needed to enforce the implementation of monitoring (Chang et al., 2015).

The aim of behavioural monitoring in IS compliance is primarily to ensure compliance with the organisations ISP (Williams et al., 2019). However, employees rarely follow ISPs, and it is very costly and simply impractical to monitor each individual (Williams et al., 2019; Herath & Rao, 2009). When it comes to access control, it is more common to check whether access rights are still appropriate rather than an employee being in possession of a document they should not have (Kirlappos et al., 2013).

Further, employees have reported discomfort with the employee monitoring policy when they perceived that there was an overuse of monitoring. Research has also shown that excessive or unnecessary monitoring leads to negative perceptions of the organisation's policies (Chang et al., 2015). If employees perceive that there are sanctions if they are caught violating the ISP, they are more likely to comply with the rules, meaning that certainty of detection has a positive impact on security behaviour (Herath & Rao, 2009). Although employees recognise the need to monitor illegal actions that can compromise security systems, employees need to be assured that their private information remains private (Chang et al., 2015). It is imperative to ensure a balance between maintaining structured monitoring and respecting employees privacy to uphold a positive relation and encourage compliance.

2.4 Theoretical framework

In short, the macroergonomic framework produced by Kraemer & Carayon (2007) highlights the distinction between accidental and deliberate causes of poor security in computer and information security (CIS), and which aims to identify and describe the work system elements contributing to human errors that may cause CIS vulnerabilities. When it comes to organisational threats, security breaches, internal problems or security effort, humans are seen and regarded as the weakest link in IS (Myrsky et al., 2009; Khan & AlShare, 2019; Aggarwal & Dhurkari, 2023; Chen & Tyrant, 2023; Jiang, 2022; Altamimi et al., 2020; Kirlappos et al., 2013; Hu et al., 2012).

The framework acknowledges that while human errors contribute to security vulnerabilities, not all violations necessarily lead to adverse outcomes. It introduces the concept of "safe violations" when coupled with a valid mental model, which can actually enhance security. The framework discusses the consequences of human errors within the CIS organisational context. It defines vulnerabilities as weaknesses in the system that allow unauthorised actions. Khan & AlShare (2019) reflects that employees are viewed as both the weakest link and the greatest asset, making compliance with ISPs and security measures critically influencing the level of success in any IS program. While organisations may invest in large scale security systems and guidelines for IS, the human element is still the pivotal role of success.

2.4.1 Human error framework

As earlier stated in this thesis, blaming individuals for errors or violations is a more common strategy than trying to figure out the underlying cause or systemic factors that contribute to them, also known as the latent organisational conditions, such as faulty equipment, management practices, or unclear procedures. Security vulnerabilities are increased by the knowledge employees possess regarding organisational information systems, and their access to sensitive data during routine work activities (Hu et al., 2012).

In the proposed framework, by shifting the focus away from the employees, one can have a more complete understanding of where the influential aspects may lie.

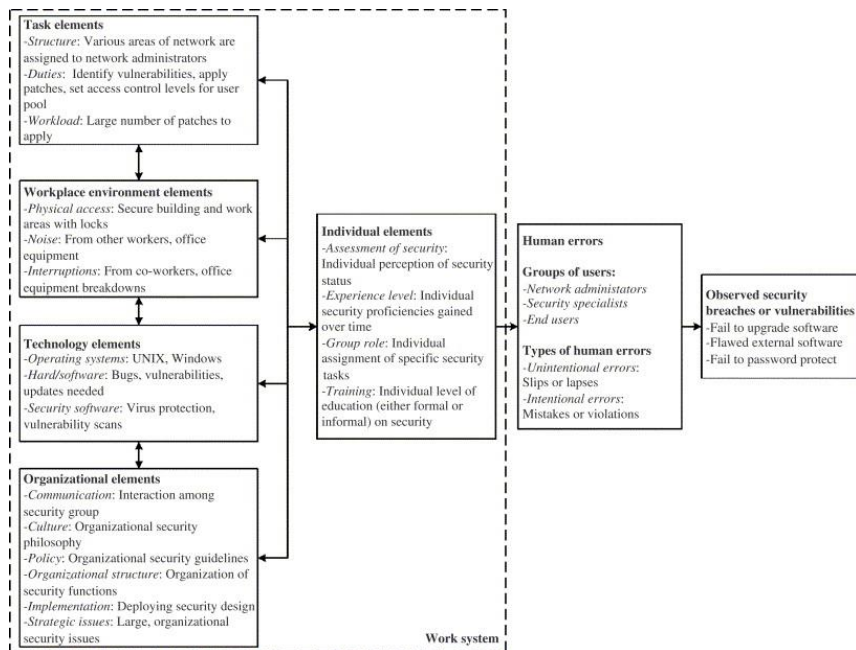


Figure 1: Illustration of Kraemer & Carayon's framework on human error

According to Kraemer & Carayon (2007), a work system can be conceptualised into five different elements: the individual, task, technologies, environment and the organisation. In the framework above, these categories make out the work system illustrated by the stippled line. While the different work system elements might be the same for all individuals, each individual will perceive the work system differently. The individual in this framework makes up an employee, how they perceive security, their experience level, significance of security in a role setting and their level of security training. These different factors may further play a role in how any human error occurs. Here it is distinguished between intended but inappropriate mistakes and slips or lapses, which are unintended actions or lack thereof.

In exploring organisational aspects of ISP non-compliance, it is crucial to consider a key distinction. While humans play a vital role in security, attributing incidents solely to human error oversimplifies the issue. Our approach recognizes humans as vulnerable links influenced by broader organisational dynamics. For instance, stress due to work pressure is an organisational element that influences an employee. The exhibited behaviour here is shaped by stress as an outcome of the organisational dynamics rather than the cause in itself. Our research methodology combines current knowledge with findings from our own research. By conducting this research, we aim to uncover insights that transcend simplistic blame. The goal is to change the above framework to better fit with the context of ISP, and aims to shift the discourse from blame to understanding and proactive change. This to empower organisations to address systemic vulnerabilities and foster a culture of security consciousness. Ultimately, our goal is to contribute to both academic discourse and practical improvements in organisational security practices.

3. Research Approach

The study's objective is to create a framework to help understand what organisational aspect influence employees compliance behaviour. Thus the study needs to address the following research question (RQ):

How do organisational elements impact employee compliance behaviours?

In the sections below, the chosen approach to the study will be discussed and the reasoning behind the decision, by describing the research design, covering the data collection, analysis and ethical considerations.

3.1 Qualitative case study approach

Qualitative research stands as having a multifaceted approach, encompassing various techniques and philosophical underpinnings that delve deep into understanding the subjective experiences, perspectives, and phenomena of individuals and groups (Tenny et al., 2022). It favours the richness and complexity of human understanding in a real-life setting over the strictness and limitations of quantitative studies. As Myers and Avison state, qualitative research is underpinned by underlying assumptions about what constitutes valid research and which methods are appropriate, be they positivist, interpretive, or critical in nature (Myers & Avison, 2002).

At its core, qualitative research prioritises the understanding and interpretation of phenomena through the meanings attributed to them by participants (Myers & Avison, 2002). It embraces the context in which these phenomena occur, acknowledging the intricate interplay of social, economic, cultural, and physical aspects in shaping individuals' behaviours and experiences. As such, qualitative researchers immerse themselves in the natural settings of their subjects, aiming to capture the nuanced intricacies that quantitative methods often overlook. In the context of ISP compliance, understanding the way behaviour and experience influence the choices employees make is highly important.

By immersing themselves in the experiences of participants, researchers can uncover novel insights and perspectives that pave the way for further investigation. Our research being related to exploring the ISP field, puts our efforts in the *exploratory* category. Exploratory research conducted within the qualitative area is "designed to illuminate how a phenomenon is manifested and is especially useful in uncovering the full nature of a little-understood phenomenon" (Hunter et al., 2019). Through immersive qualitative and inductively oriented case study approaches, scholars examine management and organisational phenomena, seeking to understand their complexity and generate knowledge (Eriksson et al., 2021). By doing exploratory research through an inductive qualitative method, resulted in an inductive case study. This way we can truly aim to explore the organisational and human behaviours and influences that drive ISP compliance.

3.1.1 Research design

The research design refers to the chosen strategy to answer the research question(s). The research question, theoretical framework, methodological approach and resources available in the study determine the choice of research design. The design should integrate the different elements of the research study in a coherent and logical way, to ensure that the research problem is addressed efficiently (Kirshenblatt-Gimblett & Trochim, 2006). It outlines the plan for data collection and analysis. Our objective requires thorough exploration within our problem area to uncover valuable insights and potentially new knowledge. To achieve this, we have chosen to pursue qualitative research for this study, as it aligns best with the nature of our project. The topic of the study evolved iteratively as we read more literature and collected data. Hence, the initial focus of trust influence on non-compliance shifted to the study of organisational elements impact on compliance behaviour.

According to Hancock et al., a case study can be split into three different case study categories; exploratory, explanatory and descriptive. The author further states that exploratory designs aim to establish the research questions for a subsequent study or assess the viability of research procedures (Hancock et al., 2021). Due to the lack of research articles published about organisational impact in the field of ISP non-compliance, we wish to continue to explore this territory through an exploratory case study. Exploratory case studies are valuable for generating new ideas, theories, or perspectives, and they can serve as a foundation for further research.

Looking at Sarker et al.'s map of genres in qualitative studies, our study falls under the exploratory case study area, see the red circle in figure 2. They state that in this genre, exploratory case studies often employ inductive reasoning (Sarker et al., 2018). Typically, these studies adopt a data-centric approach, treating data as representative facts that contribute to a realist reconstruction or recounting of events, which aligns with our aspirations for conducting this research. Through our research we aim to use the data collected together with the information unveiled in the SLR to construct possible outcomes, while also treating the data we collected from our interviewees as representative facts from our project partner organisation.

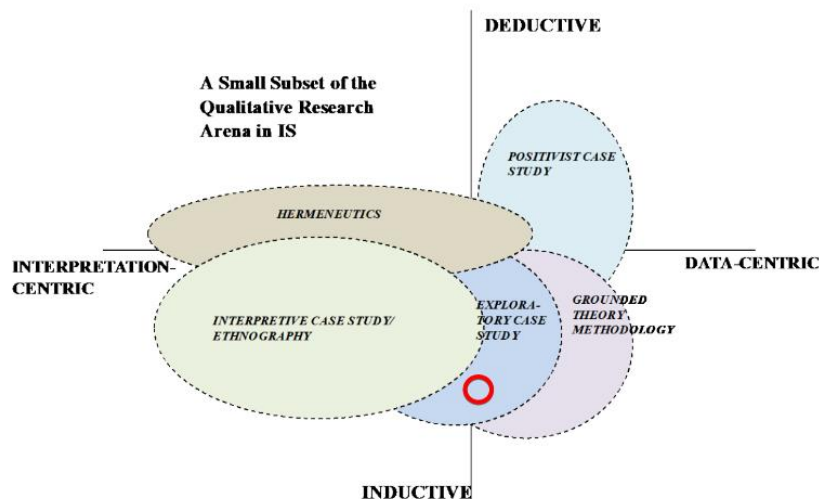


Figure 2: Map of First-Generation Genres in Qualitative Research (edited) (Sarker et al., 2018)

In essence, our research entails gathering data through transcribed interviews to develop a framework based on our findings. By employing an exploratory approach, we will leverage existing knowledge to augment interview questions and explore uncharted territory. In the end, the study's outcomes will yield a refined framework, building upon the one outlined in chapter 2.4.

3.2 Literature Review

To address the chosen research problem, a SLR was carried out. According to a paper written by Richard T. Watson and Jane Webster, “an effective review creates a firm foundation for advancing knowledge. It facilitates theory development, closes areas where a plethora of research exists, and uncovers areas where research is needed”(Webster & Watson, 2002, xiii). Conducting an SLR will allow us to justify conclusions and answers that we draw, after synthesising the research findings.

3.2.1 Method

The approach selected for conducting the SLR involves adopting the Xiao and Watson model, known for its multiple criteria and steps. This methodology consists of inclusion criteria, literature identification, data extraction, analysis, screening for inclusion, quality and eligibility assessment, and iterations (Xiao & Watson, 2017). Using this multi-step method ensures a focused research process, resulting in the extraction of highly relevant data without unnecessary information redundancy.

3.2.2 SLR criteria

To simplify the selection of scientific literature, Xiao and Watson suggest establishing a set of SLR criteria (Xiao & Watson, 2017, p. 93). These criteria serve as the fundamental basis for determining what should be included or excluded from the

comprehensive list of literature. In this SLR, only studies meeting specific criteria will be considered for inclusion. The criteria are as follows;

- The literature should be semi-recent - published after 1995.
- The literature has to be relevant to the topic at hand. It needs to focus on information security policy, compliance behaviour, security culture and trust.
- The literature should be peer-reviewed.
 - The literature should be primarily high-quality research articles (that is, published in academic journals/conferences/books)
- The literature is written in English or in Norwegian.

The reason for choosing the year 1995 as the last year to include literature from, is due to the knowledge learnt from the preliminary thesis last semester. Due to the preliminary research, it was discovered that several of the original theories and frameworks were published decades ago. Since the angle and scope was not fully established, it was advantageous to expand the scale to cover sources from an earlier year than 2013. This made it possible to incorporate more relevant literature into our SLR.

3.2.3 Search process

As part of the initial stage of Xiao and Watson's SLR methodology, the primary focus was on locating relevant literature. They outlined three key sources for literature retrieval, encompassing electronic databases, as well as forwards and backwards searches. The latter two methods aimed to uncover additional works referenced in the primary report, ensuring a comprehensive approach to gathering relevant information (Xiao & Watson, 2019). To perform backwards and forwards searches, one would have to look into the sources of the initial report, and where the initial report was used as a reference itself. The electronic databases utilised for the research purpose were Web of Science, IEEE and Scopus. These were used due to previous knowledge of them or discovered while reading research articles.

Following the initial search phase, a list of keyword combinations was created to broaden the scope for potential article inclusion. These keywords were created by exploring our scope through an initial search round where we mapped out the different topics before boiling them down to keywords and combinations.

When searching for articles, the strategy favoured keyword-based searches over complete sentences or lengthy phrases. This approach aimed to maximise the amount of search results. The keyword-combinations utilised in the literature search are detailed in table 2 below.

Topic	Keyword-combinations
Information security policy non-compliance	'Information security policy (non-)compliance' + 'tasks'/'work' 'Information security policy (non-)compliance' + 'factors' 'Information security policy (non-)compliance' + 'intentional'
Employee behaviour	'Information security policy (non-)compliance' + 'employee' + 'influence' 'Information security policy (non-)compliance' + motivation' 'Information security policy (non-)compliance' + violation'/'violate'
Security culture	'Security culture' + 'ISP' 'Security culture' + 'influence' + 'ISP'
Trust	'Trust' + 'ISP' 'Trust' + 'culture' 'Trust' + 'security policy non-compliance'

Table 2: Illustrates the search words used to find the SLR literature.

3.2.4 Screening

Reading the abstracts or synopses of the studies can further decide their relevance to the research problem, and articles that fall outside of the scope will be discarded (Xiao & Watson, 2017). This step of the literature review entails reading through the short description of the literature, before deciding if they should be included in the list for further processing.

Each piece of literature was categorised based on their short description and, if necessary, was skimmed through to determine if they would fit into this SLRs inclusion criteria. During the screening process, an extra step was added by us, using comments and a colour system in Excel to refer to the articles read. This was helpful for our discussion of which articles were to be included or excluded. The colour system consists of green=include, red=discard, orange=unsure, this in combination with our own comments on the articles helped explore the differences between what we understood and found interesting in the literature.

3.2.5 Quality and eligibility assessment

After literature was found, they were screened for inclusion and quality assessment based on Xiao and Watsons guide. Reputable publishers were deemed as high quality, meanwhile technical reports and presentations that have not been peer-reviewed were regarded as being of lower quality (Xiao & Watson, 2019). Literature found in the

previous steps was here screened again to determine if they should be included or discarded.

3.2.6 Data processing and analysis

The remaining literature that was relevant for the research problem was processed and analysed. An Excel Spreadsheet was used to keep track of every piece of literature. The data collected from each article were the author(s), year of publishing, name of the study, the main topic, a short description of the contents and how this literature is relevant to the research problem. The data that is being extracted will be analysed using NVivo, an online tool for synthesising and coding literature.

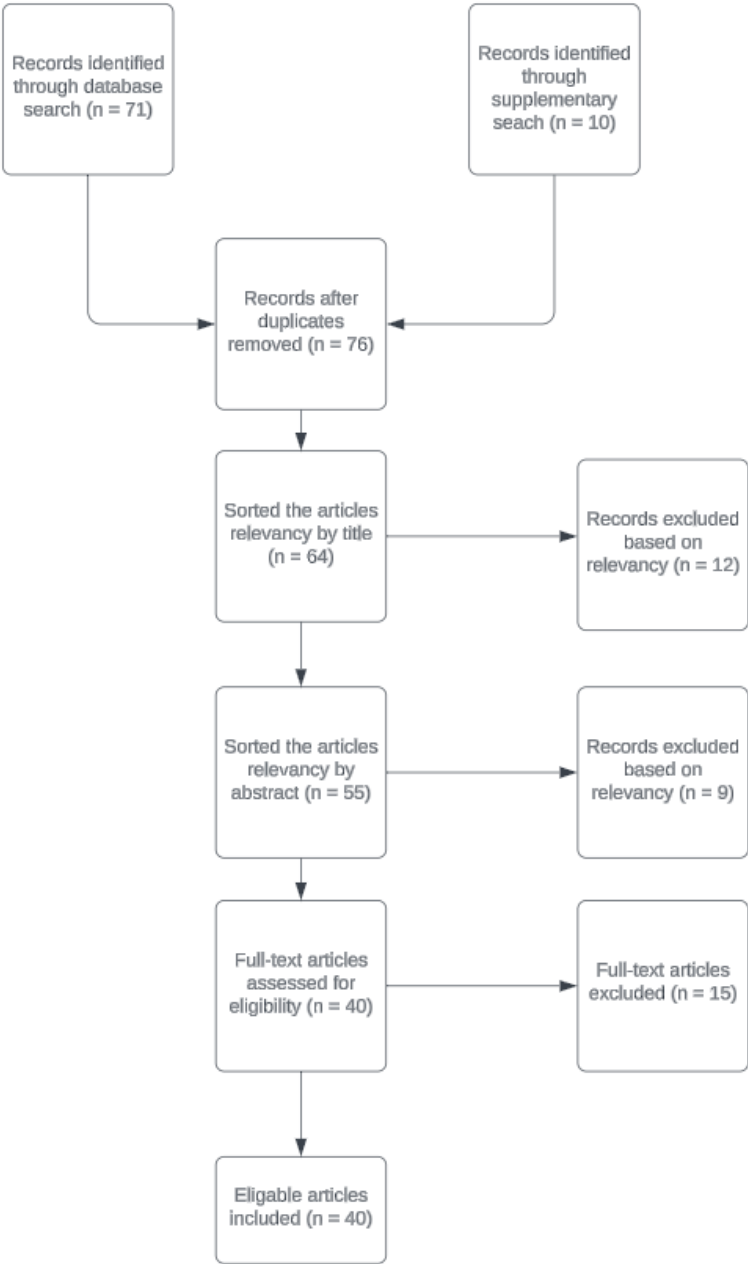


Figure 3: Systematic literature review stage overview

After completing each step of the systematic literature review, we were left with 40 eligible articles that went on to be code with Nvivo, see figure 3. While coding these articles, we kept the Kraemer & Carayon human error framework in mind. This approach guided us in categorising the literature based on whether it addressed compliance behaviour at the organisational level or the individual level. This method of classification has not been previously considered in this manner, and by applying this theoretical lens, we were able to discern that certain articles, although not explicitly focused on organisational influences, do discuss relevant aspects.

It is important to highlight that the articles we reviewed have not previously been examined through this theoretical lens. Some of these articles have not undergone extensive study or deep research and are merely mentioned in the broader literature. Our goal was to search for indications of organisational influences on compliance behaviour and to understand these influences through the lens of the human error framework.

To emphasise the scarcity of literature on organisational influences, we created a table that showcases the collected literature and categorises the content as focusing on individual influences, organisational influences, or both, see table 3. This table illustrates that there is a limited amount of research explicitly focused on organisational aspects. Consequently, we chose to include articles that, while primarily focused on individual compliance behaviour, also mentioned organisational aspects, including indirectly. This dual categorization underscores the gap in the literature, with only three articles directly addressing organisational influences. For example, certain elements, such as whether to improve policies or to correct individual behaviour mentioned by Soliman & Mohammadnazar (2022), are often discussed in relation to individuals' non-compliance. However, we have categorised ISP design under organisational influences, recognizing it as an integral organisational aspect that impacts compliance behaviour. This reclassification further demonstrates why many of the articles fall under the category 'both', and underlines the need for a more nuanced understanding of how organisational structures and dynamics influence individual compliance.

Article used from SLR (35)	Only Individual (12)	Only Organisational (3)	Both (20)
Aggarwal & Dhurkari, 2023	x		
Altamimi et al., 2020	x		
Amarkwa et al., 2018			x
Amarkwa et al., 2020		x	
Amarkwa et al., 2021			x
Amarkwa et al., 2022			x

Barstad & Sandvik, 2015	x		
Bulgurcu et al., 2010			x
Chang et al., 2015			x
Chen & Tyran, 2023	x		
Doney et al., 1998	x		
Hedström et al., 2011			x
Herath & Rao, 2009			x
Hu et al., 2012			x
Hwang et al., 2017			x
Jiang, 2022	x		
Karlsson et al., 2022		x	
Khan & AlShare, 2019			x
Khatib & Barki, 2022	x		
Kirlappos et al., 2013			x
Koohang et al., 2020			x
Koohang et al., 2019			x
Li et al., 2020			x
Luo et al., 2020			x
Myyry et al., 2009	x		
Nasir et al., 2022		x	
Niemimaa, 2023	x		
Nord et al., 2022			x
Paananen et al., 2020			x
Paliszkievicz, 2019	x		
Shadbad & Biroş, 2022	x		
Soliman & Mohammadnazar, 2022			x

Trang & Nastjuk, 2021			x
Williams et al., 2019			x
Woltjer, 2017	x		

Table 3: Reclassification of research articles

3.3 Data collection

Qualitative research acts as a comprehensive framework, connecting the various elements of human experiences, behaviours and interactions with their social settings (Tenny et al., 2022; Alsaawi, 2014). Unlike its quantitative counterpart, which relies on statistical procedures and quantification, qualitative methodologies delve into the varying complexities of individuals lives without reducing them to mere numbers (Fossey et al., 2002). This approach acknowledges the intricate nuances that shape human behaviour, allowing researchers to explore the depth and context of research areas.

There are many ways to conduct qualitative research, but the most typical technique is interviews. While methods such as observations, focus groups, and textual analysis hold their own merit, qualitative interviews stand out as a powerful tool for eliciting rich, detailed narratives from participants (Fossey et al., 2002).

Qualitative interviews provide pathways into participants' lives, offering insights into their stories, experiences, and social environments. Interviews may take on various forms, ranging from unstructured conversations to semi-structured dialogues guided by carefully crafted interview guides. For our research, we decided to conduct semi-structured interviews, as they are more focused on the explorational aspect of a topic. In addition, using semi-structured interviews makes for more openness and possibility to ask follow-up questions which will enable the researcher to get answers with depth and richness (Alsaawi, 2014; Alshenqeeti, 2014; Magaldi & Berler, 2020).

To ensure the questions we intended to ask were credible and appropriate, the first step was to review existing literature, including the human error framework (Kramer & Carayon, 2007). This created a thorough understanding of previous research findings thereby allowing us to incorporate them into the interview guide. Drawing on knowledge from the SLR enabled our interview questions to be designed to obtain valuable and relevant answers to the RQ. By using this approach, we avoided potential bias when conducting interviews, while increasing the overall reliability and validity of the study. Table 4 below presents some information about each interviewee.

Interviewee	Background	Gender
1	Manager on a project (in which SWO is a partner)	Male
2	Conducted research at SWO	Female
3	Employee at SWO affiliated company	Male
4	Head of municipal department in SWO	Male
5	Previously employed at SWO	Female
6	Data protection coordinator for SWO	Female
7	Head of municipal department in SWO	Male
8	Senior IT Advisor at SWO	Male

Table 4: Interviewee information

3.3.1 The interview process

We started contacting SWO at the beginning of January 2024, because we knew that it could be time-consuming to arrange interviews, and to give SWO information and time to prepare. It took some time to establish contact, as response from SWO took longer than we anticipated, which gave a time constraint with the number of possible interviews in the project, see Gantt chart in appendix C. However, the interviews were rich in detail and quite lengthy to make up for the small sample. Our contact person in SWO arranged interviews.

Most of the interviews were conducted digitally via the Teams application, as requested by SWO, since digital meetings required less preparation and were time-saving for the employees. This was also an advantage for us, as Teams have the possibility to record the interview and automatically transcribe it. It is not completely error-free, so it was necessary to go over and clean up errors and transcribe manually by listening to the recording. Prior to all interviews, a consent form was also sent out with information for the interviews with the request for recording, storing and using the data, see appendix B. Consent was received in writing and during recording.

However, there was one interview that was held in person, because we set up the interview with this person ourselves. This person was not employed at SWO, but had previously conducted research there. This interview differed from the others, in structure and content, as the main goal was to understand the findings they had discovered through their own research. Although similar topics were raised, the questions asked were more open-ended. This interview was also recorded, but using an audio recording feature on a phone, rather than through Teams.

All interviews started with an introduction of the interview, topics, explanation and confirmation of consent, and possibility for the interviewees to ask questions before the interview started. The interviewer would then start the interview after clarification

from the fellow student that the recording was in progress. While the interviewer asked questions from each of the five categories, the co-student noted down answers loosely and marked the main points in bold or wrote down questions for the interviewer to further address. This was to support the interviewer and to get an overview of what was said, which was particularly useful when the interviewee brought up several points in a question, as it made it easier to go back and ask additional questions. See interview guide located in appendix A.

The interviews were concluded by the interviewer asking the transcriber if there were any questions they wanted to raise, followed by a general feedback question asked to the interviewee. The interviews took between 30 minutes to one and a half hours to complete, depending on how much the interviewee addressed in each question. When an interview was completed, the interview recording was stopped and a manual check of the transcription started. The software that automated the transcription process was developed for English and Norwegian Bokmål. However, errors often occurred if the interviewee had a dialect or spoke fast.

3.3.2 Interview limitations

There are various limitations that can emerge when conducting semi-structured interviews in qualitative research. One possible limitation is that the researcher's bias may affect the results, as the researcher can steer the interviewee's answers in a certain direction and influence the findings, therefore it is essential to base the questions on collected research. Another limitation to be aware of is that the data collected may be limited to the interviewee's perspective, which may not represent the views of the organisation as a whole. To combat this it was helpful to interview people from different positions in the organisation to see if they share the same perceptions all over. There may also be issues of trust, about whether interviewees are comfortable sharing information with the interviewer, which may affect findings. Before the interviews we assured the interviewees that all information from them would be anonymized, so they could speak more freely. In addition, challenges can arise when it comes to the reliability and validity of the data, as the same questions can be interpreted differently by different interviewees, especially if they have different backgrounds, roles and knowledge. Since we were two students, it was useful to quality check with each other what interpretations we ended up with when we coded the interviews together. Finally, conducting and transcribing interviews can require a lot of time and resources, making it challenging to collect data from a large sample. To obtain the data foundation, we conducted fairly long interviews in order to really delve into the topics and the subjects' views. These limitations were considered during the interview process, before the interview guide and consent form were prepared.

3.4 Data analysis

Inductive analysis describes an approach where the researcher's interpretation of the collected data leads to the creation of a theory, framework or model (Thomas, 2006). This is in contrast to deductive analysis, where the researcher tests an existing theory. In our project, the goal is to code the interview transcripts to explore the organisational elements that impact compliance behaviour. First, the interview recordings were transcribed using Microsoft Teams and Word's transcription programme, depending on the quality of the transcription output that Teams's automatic transcriber gave. If the quality and readability was satisfactory, additional transcription happened in Microsoft Word, by uploading the meeting audio clip to further transcribe missing parts. After transcribing, the data was coded using Nvivo, which is an analysis tool that helps organise, manage and analyse qualitative data into categories or "codes". This process is in alignment with Thomas' (2006) research, which states that the outcome of an inductive analysis is the development of categories into a model or framework that summarises the raw data into key themes. The codes are created on the basis of knowledge from the SLR and what the interviewee says during the interview. This inductive analysis process assures that the research is rooted in the participants' experiences and perceptions, resulting in a more holistic understanding of the topic being researched. The findings chapter contains a summary of the responses, which are later compared with existing theories and findings from the literature review in the discussion chapter.

In Thomas' strategy on inductive analysis, there are five steps to follow: We started by preparing the raw data files, or in other words cleaning the data. This included a common format for all files, and cleaning away any interviewee identifications, like name, job title and age. The next step was to thoroughly read through the raw text until familiar with the content and had an understanding of the themes and events. The third step was to create categories based on what we had identified from the interviews, where we also relied on the themes from the SLR and made the distinction between the individual and organisational aspects. The inspiration for such a separation comes from the human error framework, so that we could apply our findings when we made our own compliance behaviour framework.

The fourth step entailed reducing overlapping codes, since a text segment can be coded in multiple categories after this process, as well as reducing redundancy between the different code categories. The final step in the process was to continuously revise and improve the categorisation system. This meant selecting a small number of summary categories that capture the most important aspects of the raw data and were considered the most important.

When we conducted the analysis, the previously mentioned five steps were followed. This resulted in the development of three key themes from the eight interview transcripts, further splitting them into smaller categories. These three core categories have underlying codes for each element that plays a role in the compliance framework

- what determines the inclusion of the various aspects in these codes depends on the context provided by the interviewee. Below in figure 4 are the three main categories extracted from Nvivo, along with the subcategories as well.

Name	Files	References
Organisational measures	1	1
Access control	8	21
Education	7	25
E-learning	3	8
Monitoring	7	20
Organisational structure	8	37
Culture	5	21
Awareness	6	22
Behaviour	2	4
Environment	7	21
Information sharing	4	5
Policy	1	5
Punishments and consequences	7	11
Technology	6	20
Top management	4	6
Trust	5	8
Work tasks	5	14
Stress	3	5
Time	7	9

Figure 4: Nvivo categories from the analysis

3.5 Ethical considerations

To conduct research for this thesis, both research data and data from interviews needed to be gathered. While the research data collected during the earlier SLR is considered "free to use," ethical considerations come into play regarding data collected from interviewees. An approval from SIKT was needed to be able to store the collected data from the interviewees, since some of the data can be regarded as sensitive or identifiable information. SIKT is the Norwegian Agency for Shared Services in Education and Research, where someone needs to be approved to be able to publish their scientific work online, as they will archive the research done (SIKT, n.d.).

This research project document does not contain highly sensitive information about the interviewees, such as their names, age, workplace or contact information, but will include a vague description of their roles. The interviewees will be informed of what data is collected about them, how it will be used and if they deem it fit, be able to revoke their consent during the project period. Any conversation or spoken discussion with any interviewee will be recorded, which was informed about before the interviews and through the consent form. After the interviews were transcribed and analysed, the recordings were deleted.

4. Findings

The organisation under study is a prominent social welfare organisation (SWO) in Norway. SWO provides services such as pensions, unemployment, child and sickness benefits. Within the organisation, millions of users are registered in their systems and thousands contact them every day for help. They have around 20.000 employees currently, divided into offices based on localisation. These offices are either part of the state or municipality, each part offering different services. Together with other organisations in Norway, SWO focuses on providing additional services to the population, reaching outside of their own possibilities to collaborate in creating additional services.

SWO recently received a report from the Norwegian Data Protection Authority about deficiencies within the organisation related to systems, access and logging. SWO itself assumed that policies and current solutions were good enough, but this has proved not to be the case. Efforts are being made to change old systems and structures to comply with laws and regulations.

As mentioned earlier our RQ is: *How do organisational elements impact employee compliance behaviours?* To answer this question, we explored the current situation in SWO, and our findings yielded inspiration and results used to create our framework. Through the interviews, we found that organisational elements such as organisational structure and measures, as well as work tasks influenced employees' compliance behaviour.

4.1 Organisational structure

In the interviews, some interviewees stated that the hierarchy structure of SWO can be challenging. The interviewees also brought up challenges they face with the environment, information sharing, the technology, management, security culture, awareness, trust implications on their compliance behaviour, and the consequences that might follow.

Hierarchy

Follow-up of regulatory standards is not just a matter of individual initiative; as interviewee 1 states, it is deeply influenced by organisational hierarchies and cultures. Prioritisation is dictated by top management rather than by individual choice.

“It is not something I handle; if it is decided that we should work on security, then we work on security. So I do not prioritise it myself, it is decided. It has to do with the hierarchy [...] It's a hierarchical culture, and that affects the working environment.”

(Interviewee 1)

Communication gaps between different departments and teams and according to interviewee 8, this can lead to potential inconsistencies or contradictions in

collaboration. Too many different orders and requirements to follow can lead to confusion amongst the employees.

“A major challenge for SWO is that the organisation is so massive, with so many different tasks and disciplines [...] Communication between departments and teams in the directorate is not always in place, which means that there may be ambiguous or contradictory guidelines from different teams [...] In addition, the SWO offices have a two-tier management, which means that they may receive different security requirements from the state and municipality, which they must deliver on.”

(Interviewee 8)

4.1.1 Environment

Through semi-structured interviews, we explored how employees feel in their physical workplace, including different office solutions and their impact on employee well-being and productivity at SWO. Through an analysis of interview material from employees at SWO offices, we look at how different aspects of the office landscape affect the working environment, the possibility to comply with ISPs and individual experiences.

General work environment

AT SWO, a sense of collaboration and dedication can be found. Many of the interviewees share the sentiment of a good workplace environment, and each facet of the organisation operates within its unique context, presenting distinct challenges and opportunities. As noted by an employee,

“The working environment is probably very variable at SWO depending on where you are.” (Interviewee 8)

Private conversations at work

Problems with headsets and communication were clearly highlighted by the interviewees. At work, multiple of the participants use a specific headset provided by SWO that are used to make private calls to users. These headsets have a tendency to pick up sound from surrounding fellow employees, and might make a conversation awkward if the user on the other end hears this, or be distracting for the employee. One of them pointed out:

“The problem is that they pick up sound. The headsets have good sound attenuation, which some people are good at using and some are less good at using. It is difficult to stay focused at work while others talk audibly. For some, this can be disturbing and for others it can be annoying.” (Interviewee 4)

Talking with users of services through such headsets might prove uncomfortable for all parties involved. One solution to this, stated by Interviewee 4, is to change the way the offices are laid out. Having a less open office space is detrimental for keeping conversations private and in compliance with confidentiality.

“It is so urgent that we just have to answer it there and then, right? Then the others, if there were others here, will want to hear what was said from me. Maybe not the other way round, but they will hear what I say in that conversation. Obviously, if you had an office, which was either a cell office or something like that, the problem would be solved, but that’s not the case here.” (Interviewee 4)

The variety in office landscapes

Unsurprisingly, the way the offices are laid out are different for each department. In a quest to optimise productivity and accommodate diverse work styles, SWO has undergone a series of transformations in office design.

“It is quite an old-fashioned office space here, with partitions and so on. But we use each other’s offices for the time being. I mean, SWO’s offices nearby are more free-seating, so there is no fixed space.” (Interviewee 1)

Interviewee 1 reminisces about the traditional layout of SWO offices, characterised by partitions and fixed spaces. However, they highlight the adaptability within the organisation, where employees utilise each other’s spaces temporarily. This can both foster collaboration, or end up being indirect non-compliance if these spaces are not universally laid out.

“Yes and no. SWO operates with an ‘area concept’ in 2019, in which it was decided that all new locations should follow [...] The offices that have not yet switched to ABW mostly have cell office solutions.” (Interviewee 8)

Interviewee 8 delineates the organisation’s gradual transition towards an Activity Based Workplace (ABW) model, initiated in 2019. While newer locations adhere to this innovative concept, older ones still rely on cell office solutions.

Challenges with the office environment

Reflecting on past challenges, there is recognition that dissatisfaction with workstation setups can escalate, emphasising the need for proactive resolutions.

“It can result in sick leave, we are afraid that we have been dissatisfied with the workstation situation, and many people want cell offices in certain departments.” (Interviewee 7)

Challenges stemming from existing infrastructure limitations are acknowledged. While the current premises may not meet optimal standards, efforts are focused on maximising available resources.

“Yes, we would like to have it that way, but we have the buildings we have, we have the premises we have, so it’s something that, for example, a bank would never have accepted, in terms of lower security, just because it has to be this way [...] But if you

are in a building that has been there for ten years, and it is as it is, will you try to make the best of it? Right now they just say that it is good enough.” (Interviewee 4)

Amidst discussions on workplace improvements, the importance of privacy and security is underscored. Design considerations include the provision of private spaces for confidential discussions, reflecting a commitment to safeguarding sensitive information and maintaining a secure environment.

4.1.2 Information sharing

Effective information sharing is paramount to SWO. Within the organisation, the municipality, county, and state agencies are all dependent on each other and need to collaborate seamlessly to deliver holistic support to individuals in need. However, the web of legislation, confidentiality concerns, and organisational boundaries often presents challenges.

“The challenge is that there are municipal, county and state services [...] we have to be very aware of how we share information across these services.” (Interviewee 1)

Central to this challenge is the delicate balance between confidentiality and collaboration. While respecting individuals' privacy rights, agencies must also ensure that essential information is shared transparently to facilitate comprehensive care.

“If you receive services from this centre, you also agree that we can interact internally here [...] we can talk about your need for 'this or that'.” (Interviewee 2)

However, the nuances of information sharing become apparent when considering the implications of withholding crucial details. In some instances, failure to disclose information can lead to adverse outcomes, underscoring the importance of transparent communication among agencies. Interviewee 3 reflects on a situation that happened at their workplace;

“[...] if there is something that could affect the youth...then it is relevant information for us before we possibly say yes to that youth...if you look at child welfare services, they have withheld information in relation to substance abuse[...] it's not good enough to withhold information because it can quickly end up being fatal for them or for others.” (Interviewee 3)

Despite recognizing the imperative of information exchange at SWO, legal constraints pose significant hurdles. Strict regulations govern the sharing of sensitive data, necessitating alternative approaches to collaboration.

“But the moment we start sending this out, we are breaking the law [...] We are not allowed to send a CV to an employer, for example. Then there are some security zone obstacles along the way that we have to figure out with these laws [...] it is not always synchronised.” (Interviewee 4)

“SWO is in a somewhat unique position...employees have relevant information about the user's case [...] but at the same time does not have the opportunity to use 'municipal' information for 'state' tasks or vice versa.” (Interviewee 8)

4.1.3 Technology

Navigating the digital landscape within SWO proves to be a formidable task, as revealed by insights from interviewees. With an extensive array of specialised systems interlinked in myriad ways, the operational intricacies are vast.

“Throughout SWO, there are around 200 specialised systems. So it's absolutely enormous.” (Interviewee 6)

Furthermore, the interviewee talks about the challenges that arise when making changes to the scale of such systems and the data held by them.

*“We have an enormous number of specialised systems and huge amounts of data, which means that changes quickly cost money and take a very long time.”
(interviewee 6)*

Arising challenges

The interviewees bring up the problems surrounding the different systems they use every day. The partial integration of the computer programs introduces risks such as incorrect data entry, due to multiple open windows for different users, making it easy to make mistakes and breach security.

*“But this means that you can have several windows open at the same time for several users, which creates a risk of entering information for the wrong user [...] and we have many computer programmes that are partially integrated with each other.”
(Interviewee 7)*

Interviewee 7 also mentioned new systems that have been developed to streamline communication and collaboration with users.

“We have a number of systems where you communicate directly with users [...] This means that we work in the same digital interface, which means that as soon as I enter enough information, the user can see it and vice versa, which has resulted in a whole new level of interactivity with users and the opportunity for even closer collaboration.” (Interviewee 7)

However, as pointed out by interviewee 2, not even this solution is challenge-free, as some users use this to their advantage to put pressure on case workers to get faster responses to inquiries not related to the activity plan, and publishing private information on a platform that might not be secure for handling such data.

“If you have, for example, a plan with follow-up by a SWO leader, there is a digital activity plan where you can communicate with your SWO leader and there are some who use the digital activity plan to get in touch with their caseworker where you should not have a direct channel for security reasons. Nothing that has to do with, for example, financial, social assistance and case processing should be in it.”

(Interviewee 2)

A good observation from the interviewees is how the systems sometimes accommodate for incorrect use, which can lead to unwanted behaviour.

“Sometimes these system designers can get a little overzealous, which means that they initiate some opportunities that weren’t meant to happen.” (Interviewee 7)

Amidst all of these challenges, efforts to fortify the systems are evident, as expressed by an interviewee. After a specific incident happened, changes were made instantaneous so that such an event would not happen again.

“Yes, physical changes have been made to the specialised system, i.e. the computer system where the error occurred, so physical changes have been made to prevent it from happening again, and very clear instructions and training have been issued.”

(Interviewee 6)

4.1.4 Top management

Interviewees stressed the pivotal role of management in prioritising security initiatives and conveying a clear message throughout the organisation.

“[...] What we need is security prioritisation from management, and a clear message from management.” (Interviewee 6)

Interviewee 8 further emphasised the managerial responsibility for continuous follow-up on security measures and ensuring employees have appropriate access.

“[...] the responsibility they have for continuous follow-up to ensure that the employees have the correct access adapted to the tasks they perform... follow up on local security instructions and compliance with these for their location and the employees there[...].” (Interviewee 8)

Interviewee 7 then highlighted the importance of regular engagement and communication regarding security measures within departments. Every October SWO partakes in the security month where phishing tests happen, which will be discussed further down in 4.2.1. Interviewee 7, being a manager themselves, feels responsible to create a workplace with even more focus on security all around the year, and not just during the security month.

"[...] we have some kind of [topic] about security once a month. We have a department meeting every Wednesday [...] Also during the security month, we have a [meeting] on security at all department meetings[...]" (Interviewee 7)

The organisational structure facilitates accessibility to management, fostering an environment where employees feel empowered to voice concerns. Having a smaller sized organisation is beneficial when it comes to this.

"[...] we have relatively small units with departments ranging from 18 to 30 employees, which means that it is quite easy to get to the manager who is often available... It's very important to protect services that you can talk to and raise issues with [...]" (Interviewee 7)

Interviewees 7 and 8 shared common ground regarding the importance of managerial oversight and engagement in ensuring security compliance.

"[...] it is also a managerial responsibility to follow up on local security instructions and compliance [...]" (Interviewee 8)

"[...] we have a fairly well-developed trustee system where you can talk to management about things that feel wrong in relation to health, security and the environment [...]" (Interviewee 7)

Centralisation of policies

Centralisation emerged as a favoured approach among interviewees for implementing security policies and guidelines. This would entail making it so every office under SWO has the same general policies.

"[...] when it is centralised, it is easier to perhaps push out policies and guidelines like that. The entire standard is centralised [...] when it is at a local level, the local offices all do what they want [...]" (Interviewee 2)

Localisation, however, presents challenges as local offices may deviate from standardised policies as it is today. Even if or when SWO enforces general rules, the local offices all deviate slightly from each other.

4.1.5 Security culture

Different challenges arise in the work environment - as many interviewees point out that there has been a lack of focus on security culture in the workplace, and that old habits are difficult to change.

"There may well have been a lack of focus on the security culture - or perhaps this has 'faded away' over time. The data protection issue has actually arisen in recent times, and then it is old habits and working patterns you have operated with for many years that suddenly turn out to be challenging." (Interviewee 8)

*“We have a security culture that is probably a bit neglected in some areas.”
(Interviewee 4)*

One interviewee mentions that since security is not the main aspect of working at SWO, it is not easily manifested in the culture, which might lead to shortcomings in the overall understanding of security.

“I have worked in a few jobs where emergency preparedness and security are number one. That is what is supposed to be the actual task. So I can see that it is not easier to create that safety culture in an office where it is not the main task, if you know what I mean. Here at SWO, it is something that they have to take care of, it is not your main job [security].” (Interviewee 4)

Further, interviewee 3 emphasises that going through the e-learning modules is a tedious task, adapting a more ‘lazy’ culture in relation to completion of said modules.

“I realise that you just ask a colleague [for help] next time [if you fail your last one], so you can get through [the e-learning modules], but I do not think people necessarily take it very seriously.” (Interviewee 3)

To combat these challenges, interviewees mention that there is an increased focus in making sure employees understand the importance of security culture.

“We have it as a theme all the time, so reflection questions all the time, ‘what do we do’, ‘what can we talk about and not’, it is a culture because we have it fresh in our minds all the time, and remind ourselves of it. It is a weekly theme in SWO, whether unconsciously or consciously, it is with us.” (Interviewee 1)

*“We have it up at regular intervals and go through [security] as a routine.”
(Interviewee 4)*

“Work is now underway across the disciplines of HR, security and privacy to demonstrate the benefits and importance of a common understanding of the security culture in SWO. Webinars and physical gatherings are being organised to improve this for all our SWO departments.” (Interviewee 8)

Another interviewee mentions that an organisation with no improvement potential is impossible, and that success will only come if the employees see the importance of security at their workplace.

“I think that an organisation that does not have improvement potential in its security culture only exists in a theoretical setting. As far as SWO is concerned, we are dependent on the security culture taking root among all employees - but that requires that they also see the benefits of it.” (Interviewee 8)

One interviewee mentions that once you have started to get into your own groove at work, and figured out how the different policies hold up against the work tasks that

need to be done, it is easy to start deviating from the expectations to work in your own way, because doing it according to the ISP might hinder them in some way.

"[...] I understand very well that those who are new follow the book [...] I think that when you have been in the system for a while, you create your own way of doing it, and then it is not always the SWO-ish way is the best way to do it, because it inhibits you in some ways." (Interviewee 3)

4.1.6 Awareness

In interviews, employees revealed a varying degree of awareness when it came to security. They addressed the opportunities they have, how they can be detected and the organisational challenges associated with this.

Employee awareness

Another interviewee recognises that they probably should have been more familiar with policies, but feels that using common sense is enough.

"Yes, maybe I have touched on it a bit, but I could certainly have been more familiar with laws and regulations. If you [would] have given me a test, I would probably fail it. I [would] probably [have] failed a written test. But again, for me, it is all about common sense. And then, of course, there is 'what makes sense for me and for you'." (Interviewee 3)

Interviewee 6 reflected on different points on various points that she believes affect the awareness level of employees.

"No, it is a lack of knowledge, a lack of data tools and combined with the time crunch, I think." (Interviewee 6)

One interviewee discusses how the organisation sends out training, and stops there, pointing out how all the responsibility is placed on the employees in whether they want to follow or ignore it.

"Because then they have done their bit, and of course it is up to us to learn from it or not. So yes, I do not know how much SWO and their managers expect or emphasise these [education] modules, but they must at least send them out to us. Then they can check that they have said that this is how we should do it, and then it is up to us to follow these rules." (Interviewee 3)

However, another interviewee said that they get a lot of value out of this training and feel confident about security.

"[...] with digital mail, suggesting what I should look out for and what I should be careful not to approve of things that come in as spam and so on. So I feel that I am pretty safe. The training we do means that there are some things that are at the forefront of my mind." (Interviewee 1)

Awareness culture

Interviewee 4 noted how they work to foster an awareness centred culture, and how they try to keep their employees aware of the security in the situations they encounter.

“Yes, you cannot know it 110 percent of the time. We just have to make sure we talk about it, right? Keep it as a topic in all sorts of contexts.” (Interviewee 4)

Awareness of monitoring

In the case of monitoring, there were varying degrees of awareness among the employees. When interviewee 1 was asked about monitoring, the interviewee answered that they knew very little about it, but that they knew you could be caught.

“I know very little about it, I know that [SWO] have access to see it.” (Interviewee 1)

At the same time, another interviewee is terrified of using their access to snoop on others, because they know it will be logged and they would get caught.

“Generally speaking, we are terrified of accessing users that are not in our portfolio because we know that all this is logged.” (Interviewee 7)

Another interviewee emphasised that snooping was uninteresting, inappropriate and an abuse of access, and that it is not the monitoring that stops him from doing it, but rather his own consciousness.

*“But firstly, it is totally uninteresting for me to know what my neighbours or youths are up to, and secondly, it is not right for me to go and use the systems to snoop on others. [...] if you do that, some SWO employee can probably see it, but that is not what stops me from doing it. It's more that it is really just an abuse of the system.”
(Interviewee 3)*

4.1.7 Outcomes of non-compliance

Multiple interviewees were aware of the risks associated with non-compliance at SWO. Although they were aware of the possible consequences of non-compliance, few had experienced or knew if this was actually the case. They also mentioned an internal system for reporting faults on themselves or each other if they discovered behaviour that was not in line with policy, but that the use of this system varied among offices.

Risk associated with non-compliance

Interviewees address the possible consequences, depending on how serious an event of non-compliance might be considered. Interviewee 1 talks about the risks associated with misuse of access to internal systems, such as snooping.

“Yes, it is a criminal offence in the extreme. You can be sentenced for it, lose your job, and there are various reactions to it. Some may receive a warning, some may lose their job, some may be reported to the police [...] If it is an extremely serious misuse of sensitive information, there’s even a prison sentence.” (Interviewee 1)

Another interviewee brings up possible consequences and is the only one who is aware that this has actually happened to someone. The actual consequences were somewhat milder than interviewee 1 assumed.

“[Possible penalties could be] dismissal, it could be taking away tasks, reducing access and so on. It was here a few years ago that we had a person added to our office who had been a manager somewhere else. Some mistakes had been made in relation to their own employees, and they had used our professional systems to check up on sick leave for their own employees. They were removed from the management position and employed in my department as a “regular worker” for a period.” (Interviewee 7)

Interviewee 8 is more aligned with interviewee 7, stating that the focus is not on punishments, but rectifying the incident, understanding why it happened and support with more training and education.

“The consequence is usually that it is rectified, while other areas that could potentially have the same factors are reviewed to see if this is a general problem or an individual case. Employees may be given guidance and training in the use of systems, guidelines and security instructions, or they may be asked to suspend the processing of personal data until the legality has been clarified.” (Interviewee 8)

Another interviewee also mentions the possible financial consequences that come with non-compliance, for which the organisation becomes responsible.

“Yes, we were initially fined, weren’t we? Of 20 million as well.” (Interviewee 4)

Report system

The interviewees mention a system in place to report and rectify internal incidents, to better explore the reasons behind why it happened, and possibly prevent it from recurring.

“Breaches are reported in the non-conformity system and form the basis for review in risk and vulnerability analyses with action plans for rectification.” (Interviewee 8)

Interviewee 4 states the procedure when a non-conformity is reported in the system and how it is handled in the organisation.

“If the guidelines are breached, the breach is evaluated and a deviation is reported. We have both municipal and state lines with us. So you consider OK, where should this deviation be reported? Then it is handled, and then [the report is] taken down.”

(Interviewee 4)

This is further supported by Interviewee 6 statements on the system and procedures, which also point out where to report more serious incidents.

“If a non-conformity is reported, it is entered as a non-conformity; if it is a major data protection breach, it is reported to the Norwegian Data Protection Authority, and then it goes down the line where it is the management who takes it, who may pass it on to the person concerned, who ensures that it is rectified and makes sure to find the reason why this is happening.” (Interviewee 6)

4.1.8 Trust

An interesting aspect brought up during the interviews frequently, was trust. Due to the previous scope of the thesis, we found it exciting to find out that trust plays a role in non-compliance, as it is not widely covered in the literature. The interviewees point out that trust was an aspect in their choice not to comply with the requirements. It was also mentioned how organisations have a certain level of trust in their employees.

Trust in each other

During interviews it was brought up how the employees have trust in each other, leading to a relaxed focus on security.

“For example, I can walk out of my office and just leave my phone and everything, without thinking about things being taken.” (Interviewee 3)

“Those who know about security make the programme, and I really trust them.”
(Interviewee 1)

Another interviewee brought up how Norway is a country with perceived high levels of trust, but at the same time, this trust has been broken due to non-compliance scandals, which can lead to trust issues within the organisation and in relation to the users of their services.

“This is also what you said about Norway having a very high level of trust, but it has also been realised that this scandal has created, what shall we say, trust issues.”
(Interviewee 2)

Another display of trust in each other, was mentioned by interviewee 3, who explained how he will share information with others, if there is built a good relation between them

of trust. He is also aware of the risks, stating that he cannot know for sure that the other person will not use the information with ill intent.

“It is easier to share information with people you know on the other end of the phone, that’s when you might sin. If it had been a brand new person, then you usually hold back. I do not know if the person on the other end is not using information for something they are not supposed to, and the same goes the other way, so it is very much about who you are talking to [trust built through relation], i.e. what names you have been given, on the other end.” (Interviewee 3)

Organisational trust

Interviewee 7 addressed how the organisation put trust in the employees, that they will adhere to the policies and only use their access for the intended use.

*“It is always emphasised that all entries [searching up a user in the system] must be motivated and that there is a need. But there is an element of trust in this.”
(Interviewee 7)*

This is also supported by interviewee 8's statements that the SWO must have trust in the employees that they will comply with the rules set by the organisation.

“As an employer, SWO has a certain dependency on trusting its employees to follow the guidelines that have been set and to comply with the framework provided by laws and regulations...” (Interviewee 8)

4.2 Organisational measures

During the interviews, aspects surrounding organisational measures, focusing on three key topics, namely education, access control, and monitoring were explored. The interviewees explained current challenges with the education strategies, monitoring and the broad access controls.

4.2.1 Overall education

Depending on the kind of position an employee has, the degree of security follow-up and learning varies. One interviewee mentions that they do not have the same kind of e-learning modules as others, whilst another brings up getting security refreshers in the different areas. The mentioned modules are said to be mandatory to complete.

“[SWO] regularly focus on data protection and such in relation to e-learning modules, and we have reviews with employees in staff appraisals. Yes, we have a security coordinator who sends out [phishing] emails and such, but [my department] does not exactly have any modules or any fixed annual or fixed security checks.” (Interviewee 6)

“There are always some seminars in relation to GDPR, and you get a refresher on it - it is always a good idea to get a refresher, because if you do not, it can quickly go very much to the right or left in relation to these rules, but. So yeah, there's always some kind of seminar or something that comes up just to refresh things.” (Interviewee 3)

“The e-learning programmes are reviewed annually and are mandatory for all SWO employees.” (Interviewee 8)

Current challenges

Even though top management states that the e-learning modules are mandatory, completing them is a hassle for some. Interviewee 3 explains that he just “clicks” the modules away or rushes through them, rarely getting anything in return, stating that he believes SWO does this to save time and resources.

“[The modules] pop up all the time, and in recent years, I have really just crossed them away, because I think it is boring as hell [...] I get nothing in return, but I understand that SWO has to send its employees through such modules. [...] maybe it is to save time that they send all our employees through it, and so they are sort of ‘done’. I realise that it can be difficult to change that, because it requires a bit more of SWO and others to spend [for example] half-day sessions on it [instead], and SWO has a very large number of employees, so there are many people who need to receive the same training. So in that sense, it is of course easier to use these modules.” (Interviewee 3)

Interviewee 7 points out that they do not know how other departments are doing security follow-ups, pointing out the security month, and stating a fragmentation of differences in security between the departments.

“It is primarily my department, so I do not really know what they do in the other departments, but I know that there are many who occasionally have a sequence on security. Especially during security month [October], there is at least one time a year when we do something. At least it is addressed properly then [...] Management has the overall responsibility [for] security.” (Interviewee 7)

The interviewees mentioned challenges they see in their everyday work, with a focus on education. Since SWO has many systems, it is challenging to learn how to use them all, as they do not have enough time to absorb all the information.

“A lot has changed. So the challenge now is to provide good training in as many professional systems and interfaces as we have.” (Interviewee 4)

“It is clear that you do not pick up everything [when starting at SWO], [before] you start working [with the systems] the next few days. [First], you learn methods and professional systems, and then about HSE and security. In a way, you do not get to think about it and digest it and, in a way, reflect on it.” (Interviewee 7)

Interviewee 4 mentions that it would be better to have professionals from outside the organisation come in to teach employees about security through work cases, enhancing the ability to learn in a 'plural' setting, in accordance with interviewee 3's views.

"I think we need to work on bringing in people from outside who are security professionals, and that they somehow take [systems we buy] and come in and deliver them to us [personally] so that all of our employees, especially new employees, temps and students, get the same training." (Interviewee 4)

4.2.2 Access control

During the interviews, several interviewees addressed the challenges of access controls today, how they are structured, and what opportunities they can create. Interviewee 7 mentioned what determines access in the system, and that it can vary on needs and location.

"Someone in the SWO office grants access and makes decisions for their employees. So there may be differences in how strictly they enforce giving access to different topics [in different offices]." (Interviewee 7)

Allocation of access

Interviewee 1 explains how controllers allocate access based on work tasks, which is consistent with what Interviewee 7 explained.

"We also have a lot of good controllers who allocate access and remove access. My experience over the past five years is that they are good at giving and taking, and allocating as needed. Our profession requires us to have a good breadth of access in order to be able to do our job, service-wise. So I feel there is a balance, I do not have free access to everything, you start in the system with limited access control, and then it is up to the controllers to expand it based on the tasks you have." (Interviewee 1)

Further both interviewee 7 and 2 explains the difference between a manager's access and a regular employee. Stating that a manager has a more broad access to people, even outside their office location, and that employees do not have access to other employees files without being granted that responsibility.

"Yes, it's handled quite strictly as I, as a manager, have access to people outside of the office, but I always have to write in a justification. The other employees don't have access to anyone other than in their office, and have limited options in relation to various topics, so it's handled quite strictly and there's a regular review of administration." (Interviewee 7)

"[...] They created a separate unit in SWO called SWO-Employee [for] all employees working in SWO. They [certain employees] are placed in the special section SWO

Employee and nobody else in SWO should be able to sit and watch a colleague.”
(Interviewee 2)

Issues with current access management

All interviewees recognised challenges with current access management, addressed criticism from the Norwegian Data Protection Authority, and future solutions. Interviewee 1 explained about a case where managers had misused access to snoop, and how this was caught, later restricted and improved for prevention.

“There was a big case here in southern Norway where many SWO managers had looked at their own employees' sick leave. It was investigated in the media, and then others started to look into it. It became a huge issue, and it helped to tighten up the regulations, so it was great that it was cleared up.” (interviewee 1)

Interviewee 3 further emphasises the possible simplicity in conducting misbehaviour when the access control allows for it.

“Because it's kind of easy to do [it] if you want to. You have the opportunity to pay out a few kroner to yourself if you want to.” (Interviewee 3)

Two of the interviewees brought up the report SWO received from the Norwegian Data Protection Authority, which addressed flaws in the access management.

“The Norwegian Data Protection Authority has stated in its report that too many [SWO] employees have extended access and that this is not good.” (Interviewee 5)

“The last thing we received from the Norwegian Data Protection Authority was about access management. [...] we have a challenge, as we have very old systems and it is difficult to just change access management from having access to each county to having access to a different data group.” (Interviewee 6)

Interviewee 8 addressed what current work is done to improve the existing access controls in SWO, to meet the requirements from the Norwegian Data Protection Authority.

“I am also involved in a project that is working to change our access management from individual accesses to 'package' accesses. The idea here is that it will be easier to administer, while at the same time a central unit in SWO will be responsible for ensuring that the content of the access package matches the tasks to be performed in the various units in SWO. Today, this is up to the individual unit and its manager.”
(Interviewee 8)

4.2.3 Monitoring

In the interviews, detection, employees opinions and different challenges associated with monitoring are addressed. According to interviewee 8:

“There are various security elements in SWO that capture the misuse of access (unauthorised access).” (Interviewee 8)

Detection

Several of the interviewees mentioned that misuse of access in the system can be detected by logging.

“No, monitoring in the systems... one knows that if you pry into something that is none of your business, it can be noticed by others; whether it is that I enter a youth I am not supposed to check or my neighbour or something else, there is a lot you can do - a lot of information you can find there as a SWO employee.” (Interviewee 3)

“[...] there is little direct monitoring of employees. What is possible is to retrieve logs that show access made to individual users, in order to detect whether unauthorised access has been made. This system is handled by the Directorate's Security Section, and access to logs is only granted on request where there is a suspicion of misuse - or where the user himself requests access.” (Interviewee 8)

“Yes, we log everything that happens on our computers. Everything from what we browse on the internet to what we access and view in the internal systems. So if I have an internal system open, everything I do, who I am looking at, what I am looking at in that person's file and so on is logged, so you can go back and check everything.” (Interviewee 6)

Current issues with logging

Interviewees raise the challenges connected to the current logging solution. Both interviewee 8 and 5 mentioned how the logging is lacking in details on why the access has occurred, and what information that was accessed.

“The challenge with logs, for example, is that you do not get information about why the individual employee has accessed them [a person], which means that you have to carry out several internal investigations to identify the reason and whether it is a matter of business need or unauthorised access.” (Interviewee 8)

“[...] the logging should have been even more detailed in terms of telling you which documents you have opened and read.” (Interviewee 5)

Another interviewee mentions how employees have to write why they accessed a person's file, and that he himself does not write why, because he as a manager has access because he has to give employee's guidance. This is quite interesting, as mentioned in chapter 4.1.7, how a manager used his access to snoop.

“[...] Some people are good at writing down that they have been involved in a case, because they know there may be questions about why [...] As a manager, I rarely write that down because as long as people who work for me have the case, it is

natural for me to get involved. But before I was a manager, I was more careful and wrote it down so that I could remember it myself.” (Interviewee 7)

4.3 Work task

Throughout the interviews, conflicts between primary tasks and security as secondary tasks were mentioned. They explained how they either have to work around security, have a lack of expertise, too much work pressure or have to disregard security in order to deliver on their work tasks.

“Then I can spend more time on what I am working on.” (Interviewee 1)

Interviewee 1 brought up that they trust the security implemented by the responsible in the organisation, and therefore focus more time on his primary tasks.

Conflict between security and work tasks

One interviewee mentions how they sometimes have non-complied to security and confidentiality, but for the benefit of the youth he is helping, and to improve collaboration between entities.

“Obviously, I am sure I have had my fair share of mishaps, but it is all about how to achieve the best collaboration for the youth [...] and that sometimes means crossing the line a little? I have been here for a while now, [...] so I have definitely crossed some boundaries in relation to confidentiality and things like that.” (Interviewee 3)

Interviewees speak on how SWO employees try to stay within guidelines, but they often feel restricted to the help they can provide, conflicting with their primary work.

“Yes, you want to stay within the bounds of security and not go beyond that, but there is also a duality when you feel that I might have been able to help further, but I know that we are not allowed.” (Interviewee 2)

“The challenges that I can often feel sometimes usually come from my own company, i.e. from SWO and the regulations they have. This can hamper me in meetings sometimes, with what we talk about, this issue of confidentiality.” (Interviewee 3)

Security as a focus

Interviewee 4 explains how it is difficult to keep security in mind when it is not seen as the primary task of a SWO employee, compared to other professions.

“I mean, if you work as a security guard or a police officer or a firefighter or whatever, that is what you do and that is your job [security], whereas here in SWO it is something you have to look after. It is not your main work task.” (Interviewee 4)

Another interviewee raises the issue of high workloads that make it challenging to focus and follow good security practices, and that SWO is aware that security could be improved

"There has probably always been a strong focus on the fact that security in SWO is not good enough, [...] Of course, we should be better at this, but the heavy workload makes it difficult to familiarise yourself with security." (Interviewee 7)

4.3.1 Time

In the interviews, almost all interviewees mentioned that time was a challenging aspect when it came to work tasks and security. Several of them emphasise how important it is to have sufficient time to perform quality work and stay within the security guidelines.

Security is time-consuming

The first interview mentions the challenge with prioritising security, when it is mostly a secondary task, getting in the way of their primary task, and recognizes that security is time-consuming.

"If it is imposed on you on a busy day, it is difficult. When you have to prioritise it, and are forced to prioritise it at a time when a manager says "it is time to make it happen", things can be difficult, at least if you're busy with other tasks, but we know it is important." (Interviewee 1)

Multiple interviewees also state that time is a limited resource, and hence will impact security.

"When time is a scarce resource, it can also mean that you do not get to work as well on security as you would have hoped." (Interviewee 7)

"In the midst of an otherwise hectic day, you suddenly have to do security training for half an hour or so. It is one of those things that you just have to get through as quickly as possible, and then I do not know how much people are left with afterwards." (Interviewee 3)

It was also mentioned that many of the challenges with time and prioritisation are linked to budget cuts, which affect what SWO and its employees are able to prioritise. It is recognised that time is important to be able to prioritise security, but that you do not always have enough.

"From experience, I would say that the most important challenges are time and prioritisation. SWO is constantly experiencing financial cuts, which means that the local offices have to prioritise their use of resources better [...] To ensure that the individual knows what to do if an incident occurs, it is necessary to prioritise setting aside time for exercises and reviewing current routines and guidelines - also when changes are made to these. As mentioned, SWO is a living organisation that is

constantly evolving, which makes it important to have sufficient time to keep up with developments in order to maintain the necessary competence of the individual employee.” (Interviewee 8)

High workload and time limitations

It was also mentioned in the interviews that there is a lot of work pressure, and several people recognised the lack of time to get everything done.

“I guess I could sometimes feel a bit of a time crunch.” (Interviewee 5)

Another interviewee talked about how SWO employees had such limited time that they could not help all the visitors who needed it. This resulted in visitors asking other civilians in the office for help, including sharing sensitive personal information with them, which in turn compromises security.

*“It was also clear that some could not get help from a SWO employee. They felt that they did not have time to sit and go through everything with the citizens. That is why they contacted others in the office, i.e. citizens, to ask for help. I would have thought that it was safer to get help from someone who worked there to look at my bank statements than from another visitor. It was often the case that the citizens themselves weren't so concerned about security and wanted help instead.”
(Interviewee 2)*

4.3.2 Organisational origins of stress

During the interviews, we found that interviewees reported stress as a persistent aspect in their work life. They mentioned that they experienced stress because of time pressure, workload, transition to digital solutions and budget cuts. Some interviewees also mentioned how they themselves take measures in their working day to minimise stress.

Increased stress due to digitalisation

When the interviewees talk about digitalisation and the new digital services, a lot of positive things come up, rewards they can take advantage of, such as cutting back on staff for certain services and relocating resources. At the same time, some challenges arise for the employees with this transition, which creates a strain of stress.

“[The activity plans] are extremely good because you can provide close follow-up, but at the same time it can lead to extra work pressure because the user can be on you constantly and ask about something. In addition, you have a response deadline of two days when a user enters something, so it can create an extra stressful situation for the employees at SWO.” (Interviewee 7)

Employees experienced more stress when they were understaffed. Even though digitalisation of services should free up time and resources, it turned out that it was not

possible to cut as much as expected, because it created more stress and negatively affected the working environment.

“SWO has also made an effort to recruit more people because when I was there and made observations, it was very tiring. Those who worked were super stressed, which affected the work environment. What has made them recruit is that they have gone from being 2.5 employees to being 4 or 5.” (Interviewee 2)

Budget cuts increased work pressure

Interviewee 7 mentions how there has been an increase in perceived stress for many employees due to budget cuts, which has resulted in an increased workload for all employees.

“I am sure a lot of people feel challenged by stress, especially since SWO cut a good number of positions in 2023, which resulted in each individual employee having more to manage. Political decisions cause SWO's budgets to go up and down, always depending on what the government will allocate to our services.” (Interviewee 7)

Interviewee 5 shared how she had to make sure a decision was not scheduled during busy periods to minimise stress for her and the recipient.

“For my benefit, to avoid finding myself in a stressful situation before going on holiday, for example, or create a stressful situation for the recipient of the benefit. I had to make sure that the resolution never ended up during some kind of holiday, vacation or other. This saved both me and the people receiving benefits a lot of stress.” (Interviewee 5)

5. Discussion

This study aimed to develop a holistic compliance behaviour framework that comprehensively captured the organisational conditions that influence individuals' actions to comply or violate the policies. We wanted to shed light on the underlying organisational elements such as work tasks, environment, technology and the structure of the organisation. These influence individuals' behaviour and decision-making when it comes to compliance. Following an exploratory research approach, we constructed a theory-informed framework in line with the human error theoretical framework, resulting in a compliance behaviour framework based on our findings.

In this chapter, we delve into the detailed discussion of our findings by presenting an in-depth exploration and analysis of the organisational elements that influence compliance, highlighting key emerging themes in our data. We aspire to present a nuanced and comprehensive understanding of compliance behaviour by integrating these insights into our holistic compliance behaviour framework. In this way, we are contributing to the existing knowledge in the field and providing more insight into the organisation's role in compliance behaviour, which is little covered to date.

5.1 Creation of the framework

Our study's contribution is a compliance behaviour framework, which incorporates the organisation's roles in compliance behaviour. As a result of the conducted SLR and interviews, the findings were compiled into a framework. The framework is inspired by the human error framework, but set in a compliance context. Our compliance behaviour framework contains the same five main elements as Kraemer & Carayon's framework, which are: work task, environment, technology, organisation, and individual. However, the underlying categories are different as our framework is composed of our findings related to compliance behaviour. The first four are the organisational elements that influence the individual element, see figure 5 below. Together these explain compliance behaviour, and the resulting consequences. The framework is intended to bridge the gap with current research, shifting the focus from the individual to also include the organisation in compliance behaviour. Our framework also includes two variations of outcomes, where we distinguish between non-compliance and compliance consequences. Interestingly, we found both positive and negative outcomes for both compliance behaviours.

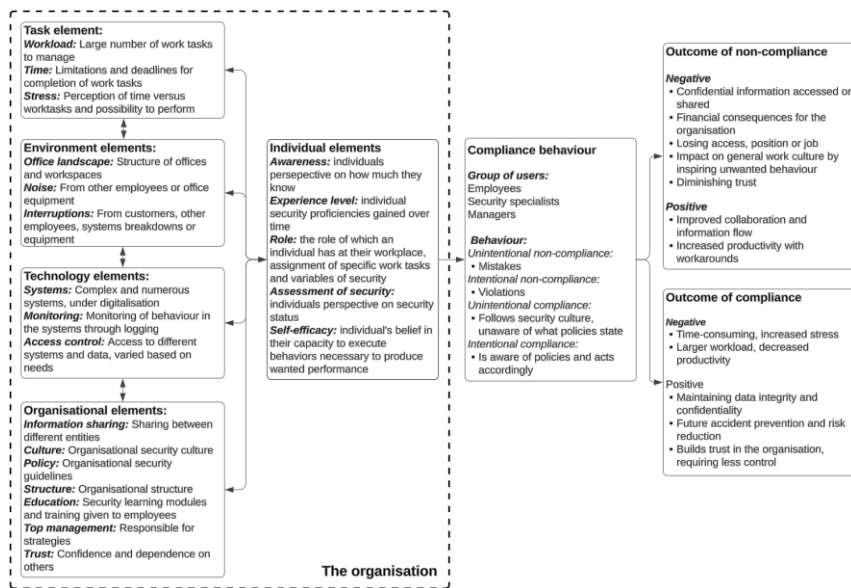


Figure 5: Illustration of the compliance behaviour framework

5.2 Implications for research

In this section, we will explore the theoretical implications, and provide a deeper understanding of the broader significance and contribution of our research. We will discuss the implications of the theories touched upon in the literature review in correlation with the empirical findings.

5.2.1 The compliance behaviour framework

The compliance behaviour framework encompasses elements from the different aspects presented in the background chapter, including the theoretical framework by Kraemer & Carayon. This human error framework influenced the process of developing our compliance framework, as they were the first to address the organisation's conditions in influencing a person's actions in the case of human error (Kraemer & Carayon, 2007). By taking the same approach, we were able to show how the organisation and past choices have led to employees' current compliance behaviour. As mentioned earlier, the compliance behaviour framework contains the same five categories as the human error framework, but contains different subcategories due to the different contexts. The subcategories are based on the collected literature and interview findings.

There were some similarities between the literature and empirical findings, where they touch upon the same aspects, but the perceptions are different. The literature mainly focuses on the human role in compliance, and how it is regarded as weakest link (e.g., Myyry et al., 2009; Chen & Tyran, 2023), while the interviewees recognise how organisational elements like leadership, hierarchy and environment impact their behaviour. Even though researchers state that organisational elements are influential (e.g., Hu et al., 2012; Hwang et al., 2017), there is a lack of visualisation of the organisational influence and how it impacts employee compliance behaviour. The

compliance behaviour framework is shown in figure 5 above. In addition, our framework includes elements like trust, information sharing, and environment, which is rarely or not at all addressed in the literature of compliance, gaining a more holistic understanding of all the elements that can influence compliance behaviour.

An important point from this study is that one of the reasons for non-compliance is that it is not clear to employees and management who is responsible for information security (Williams et al., 2019). The compliance behaviour framework helps to visualise how employees, management and the entire organisation have a responsibility for information security, bridging the hierarchical gap between them. Our framework demonstrates its validity and applicability by aligning with established theories and themes surrounding human errors in ISP compliance. By examining the data found during the interviews, against the Kraemer & Carayon framework and their categories for human errors, we can trace the origins of non-compliance from individual mistakes to systemic organisational ones. This alignment underscores the transition from viewing security lapses as isolated human mistakes to recognising them as organisational challenges.

5.2.2 Our study's contributions

What contrasts most between our findings and what the literature says about compliance is that the findings from the interviews are more related to the organisation, rather than individual aspects - which is what the literature mostly focuses on. Apart from the change of focus, and the inclusion of the organisation, there are many similarities between our findings and what the theory claims. The compliance behaviour framework is an integration of concepts - it builds on human error framework and current topics addressed in SLR, such as self-efficacy, trust, moral reasoning and policy making.

For instance, Myyry et al. (2009) state that moral reasoning is related to decisions to violate workplace policies, and that it can be understood as moral conflicts. Further, Myyry elaborates that these conflicts arise when individuals feel compelled to prioritise between fulfilling moral obligations, such as helping others, and complying with safety policies. Multiple interviewees stated that they experience being in situations where it would be simpler for them to conduct non-compliance for the sake of helping their users, in especially vulnerable situations. These scenarios often involve a conflict between following strict policies and taking actions that are perceived to be in the best interest for the user or the safety of the worker.

Although there were many commonalities between our findings and the literature, we discovered some findings that, as previously mentioned, are not well documented. We identified findings related to trust, information sharing and environment.

Trust

Several interviewees mentioned trust, both the trust between each other and the organisation's trust in the employees. Some mentioned trust as a catalyst for non-compliance, where the better the relationship, the easier it was to violate policies. Others explained how there is a lot of trust in relying on employees not to take advantage of the access they have in the systems, as SWO has a business need that sometimes requires many accesses. It was not surprising to discover that trust was an aspect of compliance behaviour, as Norway is a country with a high level of trust. As mentioned by Barstad & Sandvik (2015) and in the interviews, Norway stands out as a country with one of the highest levels of trust in the population, making it more relevant for Norwegian business to graph the role trust plays in their organisation.

The significance of understanding compliance behaviour lies in recognising the role that trust plays within an organisation. While stated in the literature that within organisations trust is an expectation that positive outcomes will result from their actions, this is not always the case (Paliszkiwicz, 2019). Trust can serve as a double-edged sword. For example, for the organisations trusting employees can strengthen the culture, requiring lower levels of monitoring and surveillance in place. Similarly distrust can lead to reluctance to cooperate, potentially hindering organisational goals (Chang et al., 2015). However, it is not just organisations' trust in their employees that needs to be assessed, but also the trust between employees.

Trust between employees can result in a more relaxed attitude towards security, or contribute to them breaking policy based on the bond they have built. For example, the more trust there is between them, the easier it is to share information that violates the policy, in favour of productivity. At the same time, it can also lead to employees leaving their phones or screens on because of the trust they have with each other. However, if that trust is broken, it will also affect their behaviour. It is important to understand how trust at an individual or organisational level affects compliance behaviour differently. While trust appears to bring benefits, it can also facilitate undesirable behaviours and attitudes. By understanding the role of trust, one can anticipate the possible outcomes.

Information sharing

Information sharing was a finding, not previously covered in the literature, in relation to compliance behaviour. Many of the challenges with information sharing at SWO are related to sharing between the municipality and the state. Such information sharing needs to be careful and well planned out, to avoid information leaks. Interviewees mentioned that they have to be very careful with information across the services they provide, which can be a stressor for many. In addition, SWO employees hold information that they cannot use due to strict rules between municipality and state. This has proved to have a negative impact on the users of SWO's services and their partners. As a result, several interviewees feel that it is necessary to break with policies

in favour of the work tasks and users, so that they can provide better help. Information sharing in such environments has shown to make it difficult to complete work tasks and still remain compliant with their work policies. The lack of well-documented information sharing practices in literature significantly impacts the understanding of compliance behaviour, particularly in complex environments in organisations. The real-world challenges employees face, such as handling sensitive information and the stress of avoiding leaks, are often underrepresented in compliance literature. This gap can obscure the tension between organisational goals and compliance requirements, where strict rules hinder effective service delivery. Understanding these dynamics is crucial for developing realistic and supportive compliance policies that align with practical needs and organisational goals.

Environment

Another finding that was not mentioned in the literature is the environmental element. Although not covered in the compliance context, this was an element addressed in the human error framework. There were a surprising number of organisational challenges raised by the interviewees on compliance behaviour, specifically related to the physical workplace, office layout, and tools they use at work. One such instance is the headsets they must use, which are soundproof in the sense that the wearer can not hear anything around them. However, the microphone attached picks up noise from co-workers, which the user on the other end then can hear. Interviewees mentioned that it is difficult to stay compliant in such open and loud environments, as you can not be discreet, making it difficult for the employees to protect confidentiality. One thing that can alleviate these problems is to change the office layout itself, but this is also a challenge. The challenge of noise and confidentiality is associated with open-landscape offices. In cellular offices, it is easier for employees to be compliant, as they can talk to the user undisturbed, without the other employees being able to hear any of the information said by the colleague. At the same time, SWO wants to invest in an activity-based workplace, which means more open-landscape offices for employees in the future. This is an example of how the choices the organisation makes can make it challenging for employees to be compliant later on.

The lack of studies involving work environment elements holds significant implications for understanding and studying compliance behaviour. When the physical elements of the workplace, such as the aforementioned office layouts and tools, are not thoroughly examined, it can conceal the practical challenges employees face in staying compliant. For instance, in SWO, the noise and lack of privacy in open-landscape offices made it difficult to protect confidentiality, directly impacting compliance. Without documentation and literature on these issues, it is challenging to develop strategies that address the real-world barriers to compliance. Understanding the role of the work environment is crucial for creating policies that support employees in their efforts to comply with regulations, ultimately leading to more effective and realistic compliance strategies.

5.2.3 Perspective change

The approach in this study is in significant contrast to the existing literature on compliance. Instead of focusing primarily on aspects that affect individuals, we have broadened the scope to also include the organisation as a whole. While also covering the individual aspects that affect employees. By adopting a broader focus, we are able to see the totality of compliance behaviour and visualise how all the different elements are connected. Although this approach is new to the compliance context, it is, as previously mentioned, used in the information security context to explain human error, and how organisational conditions play a role.

The aim from our studies is that our framework can be used by organisations to figure out where their own compliance obstacles occur. Adapting an angle where the organisation is the main focus rather than just the human element makes for a possibility to map out the underlying root causes.

The implication our framework has for compliance studies in the cognitive sense, is that it changes the existing perspective on compliance behaviour, by illustrating what the process of compliance looks like, and allocating responsibility instead of assigning blame. In this way, we are able to shift the perspective away from just the human element, to the organisational aspects that altogether influence the compliance behaviour.

5.3 Practical implications

In this section of the discussion, we will address the practical implications of the research findings into actionable insights and real-world applications. In this way, we aim to highlight how our framework can be used to solve practical challenges and inform decision-making processes. We will explain the potential implications for organisations, decision-makers, employees and other stakeholders.

5.3.1 Navigating the change from individual to organisational

The compliance behaviour framework developed through our study has significant practical implications for organisations aiming to enhance their compliance strategies and inform decision-making processes. One of the key insights is the recognition that compliance behaviour is composed not only by individual actions but also by the work task, environment, technology, and organisational aspects. This comprehensive perspective allows organisations to develop more effective compliance programs that address all these elements rather than focusing solely on individual employee training. By creating a more supportive environment that encourages compliance across all levels, organisations can foster a culture of compliance that is deeply embedded in their operations.

Using a framework such as this one to identify and mitigate compliance risks within the organisation is a practical application that can yield substantial benefits. By

understanding the various elements that influence compliance, organisations can proactively address potential risk areas. This proactive approach to risk management helps in preventing compliance breaches and safeguarding the organisation's assets. Developing and implementing policies informed by the framework ensures that compliance considerations are embedded in organisational practices. Policies should be well-crafted, effectively communicated, and supported by the organisation's infrastructure. This holistic approach ensures that compliance is not just a theoretical concept but a practical reality within the organisation.

Integrating our compliance behaviour framework into strategic planning ensures that compliance considerations are embedded in the organisation's long-term goals and strategies. This alignment helps in building a robust compliance framework that supports the organisation's growth and sustainability. Allocating resources effectively by understanding which of the elements: work task, environment, technology, organisation, need the most support to enhance compliance is favourable. Proper resource allocation ensures that compliance efforts are well-supported and that resources are used efficiently. Informing leadership decisions with insights from the framework ensures that decisions support and promote compliance across all levels of the organisation. Leaders who understand the multifaceted nature of compliance can make informed decisions that foster a culture of compliance and drive the organisation towards their perceived goals.

5.3.2 Policy design

To ensure effective security management, designing and implementing ISPs is crucial. These policies regulate employee behaviour, reducing security threats within organisations. However, as found in our SLR, traditional policy approaches often overlook the human element, leading to a disconnect between policies and actual security needs. To bridge this gap, top management should integrate employee perspectives and sanction expectations, fostering a sense of ownership and compliance. By being included in the security protection process and having their values considered in policy design, employees gain a clearer understanding of security and sanction expectations. This not only builds trust and collaboration within the organisation but also empowers employees and enhances their self-efficacy to actively contribute to a safer working environment. Moreover, policies must evolve beyond reactionary measures based on past failures, embracing evidence-based strategies and aligning with organisational processes. Contextual factors that our interviewees mention, such as organisational culture and management support must be considered to tailor policies to specific organisational needs and working environments. By aligning ISPs with organisational context and user values, organisations can develop policies that not only mitigate security risks but also promote user adherence and support organisational objectives.

IT and security professionals can leverage our insights to develop more effective and adaptable security policies. By using our framework, organisations might be able to

feasibly integrate it into their own management practices, enhancing the way they implement policies, whilst also figuring out the influential aspects and obstacles the employees face in compliance behaviour. Our findings have broad implications for the field of security management. By emphasising the importance of aligning organisational context with human capabilities, we contribute to the development of more nuanced and effective approaches to IS. This not only strengthens organisational resilience to cyber threats but also advances the overall discourse on security policy formulation and implementation.

5.4 Limitations

Qualitative studies offer valuable insights into the nuances of human experiences and behaviours. However, this kind of study does not come without challenges and limitations. For example, an analysis is primarily based on the researcher's interpretation of the data, which is subjective. The challenge with subjectivity is that it can result in different researchers drawing different conclusions from the same exact data. Furthermore, the analysis can be both time-consuming and resource-intensive, as it involves carefully reviewing and analysing large amounts of raw qualitative data, which often needs to be structured, cleaned and formatted first. Thirdly, the sample in qualitative research is typically smaller and more focused, therefore it can be difficult to apply the results to larger populations and different organisations.

The sample in our data collection consists of interviews with eight people affiliated with SWO. One aspect that needs to be considered with the sample is the interview with the former employee. We need to take what interviewee 5 says with a pinch of salt, as the person may be biased or changes may have occurred since they were employed. Therefore, we will rely only on what has been proven through interviews with current employees, but what interviewee 5 says will be used as background for claims. Interviewee 2 did research at SWO - they were also more transparent to share, however, subjectivity and bias may have played a role during their research collection and therefore it should be considered in the context of the rest of the interviews.

Since our sample size was limited and the interviews were extensive, we had the chance to delve deeply into the issues discussed, gaining a thorough understanding of the elements influencing the interviewees, their beliefs, and their perceptions of compliance. The issue of sample size warrants scrutiny, not solely in terms of its impact on generalisability but also its influence on the depth of our conclusions. While our deliberate focus facilitated in-depth exploration, a larger and more diverse sample could have provided a broader spectrum of perspectives, enhancing the robustness of our findings and making it more applicable for all organisations.

The ultimate goal has been to include elements that apply to most organisations, but some differences might exist - our framework prompts consideration of additional perspectives. While our primary focus lies within cyber security, incorporating insights

from adjacent disciplines such as psychology, sociology, or technology studies could enrich our understanding of compliance dynamics within organisations.

When it comes to data integrity, avoiding bias by conducting various research methods is detrimental. To gain a comprehensive understanding in our research, we used multiple methods for gathering our data, ensuring validity through data triangulation. There may still be shortcomings in the quality of the gathered data, either due to bias in the selection of participants or the quality of the interviews conducted, which can affect the reliability of the findings. In our research, however, we had limited influence on who to interview, it was a combination of our wishes and SWO's possibilities. The interviews were also transcribed along the way in order to assess what emerged and make adjustments iteratively.

Lastly, time constraints may have influenced the depth and scope of our study. As mentioned in chapters 3.3.1 and 3.3.2, we experienced time constraints related to communication with SWO. Given more time, we might have explored additional avenues or conducted supplementary analyses to strengthen our findings, thereby enhancing the richness and nuance of our research outcomes.

5.5 Future research

Future studies in the realm of organisational elements impacting employee compliance behaviours hold considerable potential for expanding our understanding of this complex problem area. One avenue for further research involves examining the various organisational elements that influence compliance behaviours. While existing studies have shed light on some key factors, there remains a need to explore additional dimensions of the organisational environment that may exert significant influence. This could involve conducting more extensive surveys or qualitative interviews with a larger and more diverse sample of organisations. This to build a comprehensive database of organisational aspects and their impact on compliance.

Moreover, future research could benefit from an examination of how organisational size and structure influence compliance behaviours. Large corporations may face distinct challenges and employ different strategies compared to smaller enterprises in promoting adherence to IS policies. Investigating the differences in compliance dynamics between large and small companies could uncover valuable insights into the role of organisational scale, resources, and culture in shaping employee behaviours. Such comparative studies could inform interventions and best practices tailored to the specific needs of different organisational contexts.

Additionally, future research directions may involve exploring the nuances of compliance behaviours across various industry sectors and organisational cultures. Different organisations may exhibit unique gaps and needs in their compliance efforts, necessitating context-specific approaches to address these challenges effectively.

6. Conclusion

This exploratory study aimed to provide a comprehensive understanding of compliance behaviour by including organisational elements. To achieve this goal, we used a theoretical framework based on human error and leveraged knowledge of existing literature and empirical findings, to develop a holistic framework for compliance behaviour.

We started out with the research question: “*How do organisational elements impact employee compliance behaviours?*”. In light of the compliance behaviour framework we created, we emphasise how employee compliance behaviour can be impacted. The framework offers valuable insight into the root elements that influence compliance behaviour. The insights we have gained from this thesis adds another viewpoint that is in dire need to be further explored, including themes, key elements and possible outcomes from the framework. It becomes apparent that while individual aspects of information security compliance and non-compliance have been extensively studied, there is a lack of research addressing organisational aspects in this context. Understanding the interplay between organisational policies, management practices, and the work environment is crucial for devising effective strategies to enhance information security compliance within organisations.

This thesis also makes a notable contribution to the broader research field by bridging the existing knowledge gap on how individuals are blamed for non-compliance, without including organisational elements that influence compliance behaviour. By examining the organisational elements, we contribute to a comprehensive understanding that can form the basis for future studies and interventions to mitigate non-compliance.

In conclusion, this study has provided a comprehensive understanding of the organisational elements that lead to compliance behaviour. This is achieved through a well-structured theoretical framework, insights from existing literature and empirical findings. Moreover, the compliance behaviour framework developed in this thesis sheds light on the elements that influence employee behaviours. As such, it provides a valuable framework for understanding and managing these behaviours.

References

- Aggarwal, A., & Dhurkari, R. K. (2023). Association between stress and information security policy non-compliance behavior: A meta-analysis. *Computers & Security, 124*, 2-11.
- Alsaawi, A. (2014). A Critical Review of Qualitative Interviews. *European Journal of Business and Social Sciences, 3*(4), 149-156.
- Alshenqeeti, H. (2014). Interviewing as a Data Collection Method: A Critical Review. *English Linguistics Research, 3*(1), 39-44.
- Altamimi, S., Renaud, K., & Storer, T. (2020). "I do it because they do it": Social-Neutralisation in Information Security Practices of Saudi Medical Interns. *Risks and Security of Internet and Systems, 12026*(1), 227–243.
- Amankwa, E., Loock, M., & Kritzinger, E. (2018). Establishing information security policy compliance culture in organizations. *Information and Computer Security, 26*(4), 420-436.
- Amankwa, E., Loock, M., & Kritzinger, E. (2020). A Composite Framework to Promote Information Security Policy Compliance in Organizations. *Innovation in Information Systems and Technologies to Support Learning Research, 7*(1), 458–468.
- Amankwa, E., Loock, M., & Kritzinger, E. (2021). Information Security Policy Compliance Culture: Examining the Effects of Accountability Measures. *International Journal of Technology and Human Interaction, 17*(4), 1-17.
- Amankwa, E., Loock, M., & Kritzinger, E. (2022). The determinants of an information security policy compliance culture in organisations: the combined effects of organisational and behavioural factors. *Information and Computer Security, 30*(4), 583-614.
- Barstad, A., & Sandvik, L. (2015). Deltaking, støtte, tillit og tilhørighet. *SSB Rapport*, (51), 1-100.
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly, 34*(3), 523-548.
- Chang, S. E., Liu, A. Y., & Lin, S. (2015). Exploring privacy and trust for employee monitoring. *Industrial Management & Data Systems, 115*(1), 88-106.
- Chen, X., & Tyran, C. K. (2023). A Framework for Analyzing and Improving ISP Compliance. *Journal of Computer Information Systems, 63*(6), 1408-1423.
- Doney, P. M., Cannon, J. P., & Mullen, M. R. (1998). Understanding the Influence of National Culture on the Development of Trust. *The Academy of Management Review, 23*(3), 601-620.
- Eriksson, P., Woiceshyn, J., & Montonen, T. (2021). Inductive Case Study Research with Organisations: A Framework of Collaborative Research Strategies and Intersecting

- Knowledge Interests. In *Case Method for Digital Natives: Teaching and Research* (pp. 307-321). Bloomsbury India.
- Fossey, E., Harvey, C., & Davidson, L. (2002). Understanding and Evaluating Qualitative Research. *Australian & New Zealand Journal of Psychiatry*, 36(6), 717-732.
- Hancock, D. R., Algozzine, B., & Lim, J. H. (2021). *Doing Case Study Research: A Practical Guide for Beginning Researchers* (4th ed.). Teachers College Press.
- Hedström, K., Kolkowska, E., Karlsson, F., & Allen, J.P. (2011). Value conflicts for information security management. *The Journal of Strategic Information Systems*, 20(4), 373-384.
- Herath, T., & Rao, H.R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47(2), 154-165.
- Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. *Decision Sciences Journal*, 43(4), 615-660.
- Hunter, D. J., McCallum, J., & Howes, D. (2019). Defining Exploratory-Descriptive Qualitative (EDQ) research and considering its application to healthcare. *Journal of Nursing and Health Care*, 4(1), 1-8.
- Hwang, I., Kim, D., Kim, S., & Kim, T. (2017). Why not comply with information security? An empirical approach for the causes of non-compliance. *Online Information Review*, 41(1), 2-18.
- Jiang, R. (2022). Exploring Employees' Computer Fraud Behaviors using the Fraud Triangle Theory. *Pacific Asia Journal of the Association for Information Systems*, 14(4), 100-113.
- Karlsson, M., Karlsson, F., Åström, J., & Denk, T. (2022). The effect of perceived organizational culture on employees' information security compliance. *Information and Computer Security*, 30(3), 382-401.
- Khan, H. U., & AlShare, K. A. (2019). Violators versus non-violators of information security measures in organizations—A study of distinguishing factors. *Journal of Organizational Computing and Electronic Commerce*, 29(1), 4-23.
- Khatib, R., & Barki, H. (2022). How different rewards tend to influence employee non-compliance with information security policies. *Information and Computer Security*, 30(1), 97-116.
- Kirlappos, I., Beautement, A., & Sasse, M. A. (2013). "Comply or Die" Is Dead: Long live security-aware principal agents. *Financial Cryptography and Data Security*, 7862, 70–82.

- Kirshenblatt-Gimblett, B., & Trochim, W. M. (2006). *Research Guides: Organizing Academic Research Papers: Types of Research Designs*. Sacred Heart University Library. Retrieved March 6, 2024, from <https://library.sacredheart.edu/c.php?g=29803&p=185902>
- Koohang, A., Anderson, J., Nord, J. H., & Paliszkievicz, J. (2020). Building an awareness-centered information security policy compliance model. *Industrial Management & Data Systems*, 120(1), 231-247.
- Koohang, A., Nowak, A., Paliszkievicz, J., & Nord, J. H. (2019). Information Security Policy Compliance: Leadership, Trust, Role Values, and Awareness. *Journal of Computer Information Systems*, 60(1), 1–8.
- Kraemer, S., & Carayon, P. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied Ergonomics*, 38(2), 143-154.
- Li, Y., Pan, T., & Zhang, N. A. (2020). From hindrance to challenge: How employees understand and respond to information security policies. *Journal of Enterprise Information Management*, 33(1), 191-213.
- Luo, X. R., Li, H., & Chen, Y. (2020). Understanding Information Security Policy Violation from a Situational Action Perspective. *Journal of the Association for Information Systems*, 22(3), 739-772.
- Magaldi, D., & Berler, M. (2020). Semi-structured Interviews. In *Encyclopedia of Personality and Individual Differences* (pp. 4825–4830). Springer. https://link.springer.com/referenceworkentry/10.1007/978-3-319-24612-3_857
- Myers, M. D., & Avison, D. E. (Eds.). (2002). An Introduction to Qualitative Research in Information Systems. In *Qualitative Research in Information Systems* (1st ed., pp. 2-12). SAGE Publications, Ltd. <https://dx.doi.org/10.4135/9781849209687.n1>
- Myrsky, L., Siponen, M., Pahlila, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems*, 18(2), 126-139.
- Nasir, A., Arshah, R. A., Hamid, M. R. A., & Fahmy, S. (2022). Information Security Culture Concept towards Information Security Compliance: A Comparison between IT and Non-IT Professionals. *Journal of Integrated Engineering*, 14(3), 157-165.
- Niemimaa, M. (2023). Evaluating compliance for organizational information security and business continuity: three strata of ventriloquial agency. *Information Technology & People*, ahead-of-print(ahead-of-print), 0959-3845.
- Niemimaa, M., & Niemimaa, E. (2019). Abductive innovations in information security policy development: an ethnographic study. *European Journal of Information Systems*, 28(5), 566-589.

- Nord, J., Sargent, C. S., Koohang, A., & Marotta, A. (2022). Predictors of Success in Information Security Policy Compliance. *Journal of Computer Information Systems*, 62(4), 863-873.
- Paananen, H., Lapke, M., & Siponen, M. (2020, January). State of the art in information security policy development. *Computers & Security Volume 88, January 2020*, 101608, 88(Art. nr. 101608), 1-12.
- Paliszkievicz, J. (2019). Information Security Policy Compliance: Leadership and Trust. *Journal of Computer Information Systems*, 59(3), 211 - 217.
- Sarker, S., Xiao, X., Beaulieu, T., & Lee, A. S. (2018). Learning from First-Generation Qualitative Approaches in the IS Discipline: An Evolutionary View and Some Implications for Authors and Evaluators (PART 1/2). *Journal of the Association for Information Systems*, 19(8), 752-774.
- Shadbad, F. N., & Biros, D. (2022). Technostress and its influence on employee information security policy compliance. *Information Technology & People*, 35(1), 119-141.
- Soliman, W., & Mohammadnazar, H. (2022). New Insights into the Justifiability of Organizational Information Security Policy Noncompliance : A Case Study. *Proceedings of the 55th Hawaii International Conference on System Sciences*, 1(1), 6812-6821.
- Tenny, S., Brannan, J. M., & Brannan, G. D. (2022). *Qualitative Study*. StatPearls [Internet]. <https://www.ncbi.nlm.nih.gov/books/NBK470395/>
- Thomas, D. R. (2006). A General Inductive Approach for Analyzing Qualitative Evaluation Data. *American Journal of Evaluation*, 27(2), 237-246.
- Trang, S., & Nastjuk, I. (2021). Examining the role of stress and information security policy design in information security compliance behaviour: An experimental study of in-task behaviour. *Computers & Security*, 104(13), 1-15.
- Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly*, 26(2), xiii–xxiii.
- Williams, A. S., Maharaj, M. S., & Ojo, A. I. (2019). Employee Behavioural Factors and Information Security Standard Compliance in Nigeria Banks. *International Journal of Computing and Digital Systems*, 8(4).
- Woltjer, R. (2017). Workarounds and trade-offs in information security – an exploratory study. *Information & Computer Security*, 25(4), 402-412.
- Xiao, Y., & Watson, M. (2017). Guidance on Conducting a Systematic Literature Review. *Journal of Planning Education and Research*, 39(1), 93-112.

Appendix A: Interview guide

Til praktisk intervju

Rask forklaring om intervjuet før vi begynner:

- Hensikten med intervjuet er å få en dypere forståelse av hvordan interne lover og regler hos SWO påvirker de ansatte sin arbeidshverdag. Vi ønsker å kartlegge effekten av disse reglene.
- Selve intervjuet vil dekke en liten introduksjon av din bakgrunn, forståelse av hvordan sikkerhetsreglene påvirker din arbeidshverdag, hvordan samarbeid med andre påvirkes, og din opplæring i sikkerhet.
- Det vil bli stilt noen spørsmål om hvert tema, men ta gjerne opp annen informasjon som kan være relevant som ikke er bedt om. Målet er å få oversikt over SWO og hvordan de interne prosessene er organisert.
- Vi ønsker bare å forstå og komme med bedre løsninger/forslag.
- Hvis du er komfortabel med det, så kommer vi til å ta opp dette intervjuet ved hjelp av lydopptaksprogramvare. Dette opptaket vil slettes etter at det har blitt transkribert og anonymisert.
 - Før vi begynner vil vi be deg om å nevne at du godtar at dette intervjuet blir tatt opp, og at du godkjenner samtykke.

Hvis du lurer på noe før vi begynner, er det tid til det nå, hvis ikke begynner vi :)

1 Introduksjon

Hvor gammel er du?

Hva slags utdanning har du?

Hvilken ansvar har du i stillingen din?

Hvor teknisk kyndig vil du si at du selv er?

2 Opplæring

Hadde du opplæring i IT sikkerhet da du først startet hos SWO, og hva gikk denne ut på?

Følte du at du fikk tilstrekkelig med opplæring om sikkerhetsregler?

Skulle du ønske at du hadde påvirkningskraft på denne opplæringen?

Har SWO noe oppfølging eller oppfriskning rundt IT sikkerhet med deg nå i senere tid? Dette kan være moduler du må ta, phishing-tester eller retningslinjer om hvordan du skal behandle sensitiv informasjon.

3 Arbeidsoppgaver

Finnes det noen utfordringer ved utføring av arbeidsoppgavene dine? (Da mtp sikkerhet, tid, stress, arbeidsmengde, informasjonsflyt & personvern)

Hva gjør du om du møter en utfordring?

Hvordan oppstår disse situasjonene?

Hvilke tanker hadde du da dette skjedde?

Hva ble konsekvensene av denne konflikten?

Kan du tenke deg en grunn til at du hadde valgt å ikke prioritere sikkerhet? (Trade offs)

Begrenser noen gang sikkerhet servicen/hjelpen du kan gi til en bruker?

Føler du at du får gitt innbyggere/brukere tilstrekkelig med hjelp?

Hva skal til for å gjøre dette bedre?

Har digitaliseringen på arbeidsplassen bidratt til noe?

Er det lagt opp til samarbeid med arbeidsoppgaver?

Kommer dette i konflikt med IT sikkerhet eller personvern?

Kan du ta oss gjennom en saksbehandlingsprosess/arbeidsoppgave fra start til slutt? (Systemene du må gjennom, tankene du har om det, tidsbegrensning, utfordringer du møter på)

Merker du deg noen steg i prosessen, det kan være forbedringspotensial?

4 Miljø og kultur

Hva synes du om arbeidsmiljøet i SWO?

Er kontorlandskapet lagt opp til arbeidsoppgavene du gjør?

Har du et privat sted du kan gå for å snakke om sensitiv informasjon?

Er du kjent med begrepet "sikkerhetskultur"?

Hva er dine tanker om sikkerhetskulturen i SWO?

Er det noen forbedringspotensial?

Har den alltid vært sånn, evt hva har blitt gjort for å endre den?

Hvordan føler du at du bidrar til denne kulturen?

5 Sikkerhet

Hvor kjent er du med de spesifikke retningslinjene for sikkerhet på arbeidsplassen din?

Hvordan påvirker disse retningslinjene dine daglige aktiviteter?

Hvilke ferdigheter har du, som hjelper deg å følge sikkerhetsreglene?

Hvordan vet du at du oppfyller kravene til sikkerhetsreglene?

Fra ditt perspektiv, synes du det er lett eller vanskelig å tilpasse deg til sikkerhetsreglene?

Føler du at mengden tilganger du har til systemene er nødvendige for å utføre arbeidsoppgaver?

Er du bevisst på hvor mange tilganger du har, og er det noen som burde vært mer begrenset? Hvorfor/Hvorfor ikke?

Hva vet du om overvåkning i SWO?

Hva er dine tanker om monitorering/overvåkning av dine handlinger i systemene til SWO?

Vet du hva potensielle konsekvenser av å bryte med retningslinjene er?

Vet du hvordan du kan få mer informasjon om sikkerheten på din arbeidsplass?

Til teknisk intervju

Rask forklaring om intervjuet før vi begynner:

- Hensikten med intervjuet er å få en dypere forståelse av hvordan interne lover og regler hos SWO påvirker de ansatte sin arbeidshverdag. Vi ønsker å kartlegge effekten av disse reglene.
- Selve intervjuet vil dekke en liten introduksjon av din bakgrunn, forståelse av hvordan sikkerhetsreglene påvirker din arbeidshverdag, hvordan samarbeid med andre påvirkes, og din og andre ansattes opplæring i sikkerhet.
- Det vil bli stilt noen spørsmål om hvert tema, men **ta gjerne opp annen informasjon som kan være relevant som ikke er bedt om**. Målet er å få oversikt over SWO og hvordan de interne prosessene er organisert.
- Dette dokumentet vil slettes etter at det har blitt omskrevet og anonymisert.

1 Introduksjon (Korte svar)

Hvor gammel er du?

Hva slags utdanning har du?

Hvilken ansvar har du i stillingen din?

Hvor teknisk kyndig vil du si at du selv er?

2 Opplæring

Hva gikk sikkerhetsopplæringen din ut på og var den tilstrekkelig?

Har SWO oppfølging rundt IT sikkerhet med deg i senere tid?

Hva er etter din erfaring de viktigste utfordringene for å sikre at de ansatte følger sikkerhetsreglene på arbeidsplassen?

3 Arbeidsoppgaver

Oppstår det noen ganger utfordringer mellom de ansattes evne til å utføre arbeidsoppgaver og SWO sine regler for sikkerhet og personvern?

Hvordan kan dette løses og hvorfor oppstår slike utfordringer?

Er det tilrettelagt for samarbeid mellom ansatte, og kan dette komme i konflikt med sikkerhet og personvern til brukerne av SWO sine tjenester?

4 Miljø og kultur

Hva synes du om arbeidsmiljøet i SWO?

Er kontorlandskapet lagt opp til arbeidsoppgavene de ansatte gjør?

Hva er dine tanker om sikkerhetskulturen i SWO?

Hva har blitt gjort for å endre den?

Er det noen forbedringspotensial?

Har det skjedd noen endringer etter at Datatilsynet sin sak kom ut?

Hvordan føler du at du bidrar til denne kulturen?

5 Sikkerhet

Hva mener du er avgjørende for å sikre compliance (samsvar) med organisasjonens sikkerhetsretningslinjer (lover og regler)?

Kontrolleres det om de ansatte er compliant med lovene og reglene for sikkerhet? I så fall hvordan?

Hvordan identifiseres non-compliance hos SWO?

Hvilke faktorer er det som oppdages?

Hva blir konsekvensene?

Hva har gjort at det har skjedd tidligere?

Kan du forklare hvilke typer monitorering dere har i SWO?

Hvordan får dere oversikt over de ansattes atferd i systemene deres?

Hva er dine tanker om monitorering og logging i SWO?

Føler du at dette er tilstrekkelig mtp. personvernregler?

Er det noe mer du ønsker å tilføye så kan du legge det under her:

Appendix B: Consent form

Vil du delta i forskningsprosjektet

'Masteroppgave om sikkerhetspolitikk'

Formålet med prosjektet

Dette er et spørsmål til deg om du vil delta i et forskningsprosjekt hvor formålet er å:

- Undersøke hvordan ansatte opplever sikkerhetspolitikken i en bedrift, både for de som står bak selve sikkerhetspolitikken, men også de som bruker de regler og begrensninger som står beskrevet i denne.
- Dette er en mastergradsoppgave skrevet i samarbeid med SWO Agder og med veiledning ved Universitetet i Agder.
- Data som blir innhentet i intervju vil bli anonymisert og lagret frem til prosjektets slutt, som er 7. juni, før det blir arkivert.

Hvorfor får du spørsmål om å delta?

Du får denne forespørselen fordi

- Du har blitt utnevnt som en potensielt viktig person i vår undersøkelse av våre samarbeidspartnere ved UiA og SWO. Samarbeidspartnerne ble spurt av oss om hvilke personer det var mulighet å komme i kontakt med, som kunne ha svar på de spørsmål vi ønsker å stille.
- Vi har fått kontakt med deg grunnet din bakgrunn hos SWO.

Hvem er ansvarlig for forskningsprosjektet?

Det er Camilla Wessel Frøhaug og Amalie Widvey som er ansvarlige for dette forskningsprosjektet. Kontaktinformasjon til begge finner du lenger ned i dokumentet.

Det er frivillig å delta

Det er frivillig å delta i prosjektet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Hva innebærer det for deg å delta?

- Gjennom et personlig semi-strukturert intervju vil vi stille deg spørsmål knyttet til sikkerhetspolitikk, arbeidskultur, arbeidsprosesser og tillit.
- Her vil vi spørre deg om alder, kunnskapsområde og arbeidsposisjon
- Det er fortsatt relevant for oss å kunne intervju deg selv om du ikke kan mye om tema(ene).
- Intervjuet vil bli tatt opp med lydopptak for at det skal kunne bli transkribert.

Kort om personvern

Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrevet. Vi behandler personopplysningene konfidensielt og i samsvar med personvernregelverket. Du kan lese mer om personvern under*.

Med vennlig hilsen

Marko Ilmari Niemimaa
(veileder)

Camilla Wessel Frøhaug
(Student)

Amalie Widvey
(Student)

LES MER:

Utdypende om personvern – hvordan vi oppbevarer og bruker dine opplysninger

- Personer som vil ha mulighet til å kunne aksessere de opplysninger du oppgir under intervju er studentene som skriver denne oppgaven og veileder for masteroppgaven ved UiA .
- Personlig informasjon som du oppgir, slik som alder og arbeidsstilling, vil bli erstattet med plassholdere (placeholders). I tillegg vil dataene lagres på en passordbeskyttet database.
- Det vil ikke være mulig at du er gjenkjennbar i den fullstendige publikasjonen.
- Det er vi, Camilla Wessel Frøhaug og Amalie Widvey, som vil lagre, behandle, anonymisere og bruke den informasjonen du oppgir.

Hva gir oss rett til å behandle personopplysninger om deg?

Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra Universitetet i Agder har personverntjenestene ved SIKT – Kunnskapssektorens tjenesteleverandør, vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Dine rettigheter

Så lenge du kan identifiseres i datamaterialet, har du rett til:

- å be om innsyn i hvilke opplysninger vi behandler om deg, og få utlevert en kopi av opplysningene,
- å få rettet opplysninger om deg som er feil eller misvisende,
- å få slettet personopplysninger om deg,
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger.

Vi vil gi deg en begrunnelse hvis vi mener at du ikke kan identifiseres, eller at rettighetene ikke kan utøves.

Hva skjer med personopplysningene dine når forskningsprosjektet avsluttes?

Prosjektet vil etter planen avsluttes 7. juni.

Opplysningene vil da arkiveres sammen med fullstendig masteroppgave, og data som er sensitiv vil anonymiseres. Rådata som er lagret i databaser o.l. vil slettes..

Spørsmål

Hvis du har spørsmål eller vil utøve dine rettigheter, ta kontakt med:

Veileder:

Marko Ilmari Niemimaa

E-post: marko.niemimaa@uia.no

Telefon: +47 38 14 18 42

Prosjektansvarlige studenter:

Camilla Wessel Frøhaug

E-post: camillaf@uia.no

Telefon: +47 41 48 71 69

Amalie Widvey

E-post: amaliew@uia.no

Telefon: +47 90 10 85 80

Vårt personvernombud:

UiAs Personvernombud

Kontaktperson: Trond Hauso

E-post: Personvernombud@uia.no

Hvis du har spørsmål knyttet til SIKT's vurdering av prosjektet, kan du ta kontakt på e-post: personverntjenester@sikt.no, eller på telefon: 73 98 40 40.

Jeg har mottatt og forstått informasjon om prosjektet Masteroppgave om sikkerhetspolitikk, og har fått anledning til å stille spørsmål. Jeg samtykker til:

- å delta i intervju
- at mine personopplysninger lagres frem til prosjektslutt og arkiveres etter, kryptert

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet

Appendix C: Gantt chart

