Merging Information Security Policies - Requirements and Best Practices

Paul Lackner

MASTERARBEIT

eingereicht am

University of Applied Science Masters Program

Information Security Management

in Hagenberg

im Juli 2024

Advisor:

FH-Prof. Dr. Harald Lampesberger, MSc

Declaration

I hereby declare and confirm that this thesis is entirely the result of my own original work. Where other sources of information have been used, they have been indicated as such and properly acknowledged. I further declare that this or similar work has not been submitted for credit elsewhere. This printed copy is identical to the submitted electronic version.

Hagenberg, July 2, 2024

Paul Lackner

Contents

Abstract

Merging information policies in an organisation may be a difficult project. Merging policies may have various motivations, e.g. to create a more efficient organisation or to merge multiple subsidiaries and therefore having a need for a consolidated policy. To successfully complete a merger of policies, strategy needs to be developped that considers these questions: What are the business goals, what are the requirements to the policies and the policy system, what is the goal that needs to be reached through the policies and who are the stakeholders of the policies? A critical part of the merger is the communication of the policy change. This thesis describes the very basics of risk management and IT operations to have a unified understanding of the topic. It further creates a hypothesis and theory on how to do a successful merger and therefore on how to communicate change of an information security policy effectively to the relevant stakeholders. The various preconditions of this merger (why it is done), are not evaluated and described but rather the doings and the results of it. Later on, an experiment is described an analysed, which will also serve as a basis for a conclusion about it and tries to evaluate the hypothesis. It will conclude that a change of a policy needs to be announced to relevant people via personal message in their own language via a suitable messenger.

Kurzfassung

Die Zusammenlegung von Informationspolitiken in einer Organisation kann ein schwieriges Projekt sein. Die Zusammenlegung von Richtlinien kann verschiedene Gründe haben, z. B. die Schaffung einer effizienteren Organisation oder die Zusammenlegung mehrerer Tochtergesellschaften und damit die Notwendigkeit einer konsolidierten Richtlinie. Um eine Fusion von Politiken erfolgreich abzuschlieSSen, muss eine Strategie entwickelt werden, die folgende Fragen berücksichtigt: Was sind die Unternehmensziele, welche Anforderungen werden an die Richtlinien und das Richtliniensystem gestellt, welches Ziel soll durch die Richtlinien erreicht werden und wer sind die Interessengruppen der Richtlinien? Ein entscheidender Teil der Fusion ist die Kommunikation der Änderung der Politik. In dieser Arbeit werden die Grundlagen des Risikomanagements und des IT-Betriebs beschrieben, um ein einheitliches Verständnis des Themas zu erreichen. Darüber hinaus werden eine Hypothese und eine Theorie aufgestellt, wie eine Fusion erfolgreich durchgeführt werden kann und wie die Änderung einer Informationssicherheitspolitik den relevanten Stakeholdern effektiv mitgeteilt werden kann. Die verschiedenen Voraussetzungen für diese Fusion (warum sie durchgeführt wird) werden nicht bewertet und beschrieben, sondern vielmehr die Durchführung und die Ergebnisse der Fusion. Später wird ein Experiment beschrieben und analysiert, das auch als Grundlage für eine Schlussfolgerung darüber dient und versucht, die Hypothese zu bewerten. Es wird die Schlussfolgerung gezogen, dass eine Änderung der Politik den betroffenen Personen durch eine persönliche Nachricht in ihrer eigenen Sprache über einen geeigneten Boten mitgeteilt werden muss.

Chapter 1

Introduction

1.1 General remarks

Information security in an organisation relies on external and internal policies and regulations stating various demands and guidelines to be fulfilled. To create internal policies to establish a risk management, the demands of the organisation need to be understood and combined with the external regulations [67][51][7] and policies (e.g.: GDPR [18][71], Cybersecurity Act [16][39], NIS Directive [19][55]; ISO 27000 family [26][52][27], NIST-SP 800-53 [57][42], ISO 31000 family [28][5], ISO 9000 [29][8]). These internal policies are the guidelines to implement information security into this very specific organisation. To change policies, the process of defining (understanding and defining the needs of the organisation, evaluating the regulations), checking, approving, and publishing a policy needs to be redone. Also, policies need to be implemented, which takes time in order to be effective. For example, a long established policy may lead to a stable technical and organisational implementation of it, while constant changing of a policy will probably lead to a partial implementation on technical and organisational level only, which may result in various stubs of policy implementations, not necessary coherent to each other.

Merging a policy may be necessary due to internal (e.g.: merging two companies or different organisational divisions) and/or external (e.g.: law changing) circumstances. When merging two or more relevant information security policies of an organisation, a lot of organisational and technical work needs to be done. Merging the policies focuses mostly on making the processes more efficient and removing duplicates in management and operations, but may also have different reasons to proceed. To achieve this, all policies need to be understood and re-evaluated including the different working cultures [38], the resources (knowledge, workforce, inventory, etc.) need to be assessed and possible blind spots need to be detected. This thesis will focus on the possible merge of two or multiple information security policies inside the same organisation and the possible impact on the organisation and relevant departments inside the organisation. This thesis regards departments as organisational areas inside organisations.

1.2 Problem Description

Merging two or more information security policies requires a complete understanding of organisations and their needs. Two different policies addressing the same topic may have been created for a completely different use case, scope, and environment. This case study is about an organisation with completely separated departments in terms of the information security policy framework and its scopes. The organisation decided to merge these departments, with the consequence, that the information security policy frameworks lost their scope and are overlapping in scope and responsibilities. Also, old structures have not been adapted. This also leads to overlapping responsibilities. For example, when merging risk management policies, the existing policies may range between being very similar to not having any similarities at all. There is a technical part as well as an organisational part.

The problems, as already described, are as follows:

- identifying the correct scope for the written policies
- difficulties to train users and administrators to work with another mindset regarding responsibilities and abilities
- completeness of the inventory and availability of all necessary data
- finding, identifying and evaluating blind spots in the departments, which should not get buried during and after the merge

1.3 State of the Art

The state of the art about merging information security policies is rather scarce. There is enough information about management itself, creating, maintaining and destroying security policies, but there is no comprehensive, recognised work on merging them. Available research work is either outdated or solely on a technical basis (e.g. merging access control lists), or both (e.g. [4]).

The need to merge security policies most likely roots from changed security requirements of the company and/or protected data which has not been brought to considerations in academic or public available industry research. A challenge for this thesis is to check if a mapping of the measurements from the technical research could be transited to the organisational part of security policies and if the outdated work still applies. Related work is located in chapter 3.

1.4 Goal of the Thesis and Methodology

The goal of the thesis is to answer the question if a merge of two policies may be efficient and what the requirements are to achieve it. The research will be done in an applied, exploratory, inductive way. It will create a guideline on what to consider when merging policies which may be reused in similar scenarios. It focuses on the change, respectively the communication of change. What are the required parameters of the change communication to effectively educate employees and implement the changed policy framework into the workflow? Research data will get acquired from public sources as well as from a representative local company, which will also be used to test the theory

and perform a case study to support the theory. This thesis does not focus on the problem of not adapted structures. This thesis focus on the communication of change.

1.5 Research Questions

The main research question of this thesis is as follows:
What are the requirements in communication for a successful and economically efficient policy change? Therefore, how to manage a successful merger. This thesis addresses multiple methods to communicate the change and will compare them. This analysis and comparision will be used to determine a strategy to successfully announce changes of information security policies.

To determine a successful and economic efficient merge, there is also the question on what and how to measure the merger, therefore:
What are the adequate measurements to measure a successful and economical merger?

1.6 Thesis Structure

The thesis will be structured the following way: Chapter 2 explains the basics, which are required to know to understand the thesis, including the terminology, risk management, and Information Technology (IT) operations and service quality. Chapter three introduces related work and what has been done before. Chapter four describes a possible theory and a hypothesis including metrics, while chapter five describes the current situation of the organisation, the case study design, the gathered metrics, and the analysis of these metrics. Chapter six includes any closing remarks and a conclusion.

Chapter 2

Basics

This thesis is about merging different information security policies into one. To be able to follow the work of the thesis it is fundamental to get an understanding of the basics of the topic which will be explained in this chapter.

2.1 Terminology

The following subsections explain the crucial terms concerning information security policies. This terminology is being done to get a consolidated understanding of the terms, so that it is clear what the thesis is about.

2.1.1 Safety

The terms *security* and *safety* often get mixed up, but have different meanings. Safety derives from the latin word *salvus*, meaning "in good health". A definition of safety is "the condition of being safe from undergoing or causing hurt, injury, or loss" [54]. Safety in terms of IT and Operational Technology (OT) means the protection from physical injuries to life due to machinery. Safety ranges from passive to active measurements; e.g.: ranging from isolating power cords of a machine as a protection from electric shocks over designing machine locations in accordance with emergency evacuation plans to the *Three Laws of Asimov* especially including the first one: "A robot may not injure a human being or, through inaction, allow a human being to come to harm" [3], which get more important with the rising usage of automated assistance in daily life (e.g.: self-driving cars [50]).

2.1.2 Security

Security derives from the words *se* which means without and *cura* which means care or to be concerned [45]. Security management and technology first tried to prevent incidents and their outcomes. Later on, new techniques tried to detect and limit security incidents that could not be prevented, as well as other techniques try to tolerate attacks but continue to deliver critical services, therefore increase the resilience of systems overall. Security is defined as a weak-link system property [45]. That means that the system is as strong and efficient as its weakest participant. Security also means to balance

between the need of securing something and the costs to do so [44], therefore it is about establishing a risk management in the defined context and scope. Modern definitions distinguish between computer or IT security, data security, information security and cyber security. In comparision to safety, security in terms of IT and OT means the protection of machinery, data and information, and systems, therefore objects.

Information security is defined by the International Organization for Standardization (ISO) as the preservation of the confidentiality, integrity and availability of information [34]. This is often referred to as the Confidentiality, Authenticity, and Availability (CIA) triad of information security. The ISO standard defines information of any kind; written on paper, saved in electronic files, spoken information and memorised knowledge, as well as any other similar kind of knowledge [69]. This definition has been enhanced as information security is "the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information" [70]. Confidentiality, integrity, and availability should be treated equally important in most cases [69], as well as there are cases in which one of these characteristics is not equally important. In OT security, integrity and availability are important to correctly operate machines, but confidentiality is not a high priority goal [36]. However, confidentiality loss occurs if a successful, unauthorised access on the system happens [69]. The goal of information security is defined as ensuring business continuity and limiting business damage by incidents [66]. Information security is also defined as information risk management [6]. Risk management is defined as a framework that will allow to handle risk and uncertainty [11]. Information security as risk management focuses on planing availability of essential IT services.

Information security addresses computers, data, as well as the people involved [47]. People, especially employees are referred to as the weakest link in information security [63], therefore, periodic information security training should be applied to administrators, developers, as well as any other personnel dealing with classified information [1]. Therefore, information security addresses IT systems and people as a vulnerability towards information.

Information security is seen as a process instead of technology [56], although it may require using chosen products [72].

Computer security or *IT security* is seen as part of information security and in a strong relationship with data security [45]. IT security does focus on securing information processing machines. The ISO defines it as defining, achieving, and maintaining confidentiality, integrity, and availability, non-repudiation, accountability, authenticity, and reliability of information assets [33]. This means securing these machines against unauthorised physical as well as remote access. Correct configuration of IT systems is key to achieve IT security. Also, an important part of IT security is the correct use and implementation[1] of cryptography [44].

As companies shift their services towards a cloud environment and cheap Internet of Things (IoT) devices flood the market, modern definitions of IT security slightly differ to older established ones as they have a different focus [22]. This introduces the term *cloud security* with its principle of "shared responsibility". Cloud providers are able to limit physical access to an absolute minimum, as well as isolate various tenants to a

[1] https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/

level as agreed in the terms between the provider and the customer. The customer is still responsible for the management of the information. Also, using of cloud services creates new attack surfaces, which need to be adressed.

IoT devices are often very limited in their configuration and are built "to just work", therefore, a focus should be laid onto the software security itself, their architecture and whether the manufacturer seems trustworthy [68].

IT security is also defined as a summary of "risk assessment, technology architecture, and policies and procedures" [9].

One of the first comprehensive explanations of *data security* defined it as a set of access, flow, inference and cryptographic controls [10]. Access controls are defined to limit access to users and processes to modern Create, Read, Update, Delete (CRUD) operations. Access controls (Authorisation) strongly relates to a working authentication process. Authentication proves an identity, while authorisation grants access to a resource [43]. Flow controls strongly relate to access controls [10]. Flow controls ensure that users or processes which are subject to a data transfer are eligible to access these data. They ensure the compliance of data classification. To create correct working flow controls is still a major problem in modern security concepts. Another control, inference control, is about limiting data acquisition by summarised data through extended knowledge. When applying inference controls the corresponding flow controls will be suspended as summarised data is intended for a greater range of receipients than detailed data. Cryptographic controls ensure that data is not manipulated or disclosed to unauthorised personnel, if all other controls are out of order (data on an external drive, faulty hard or software, etc.). This early definition already implements the principle of least privilege. Data security strongly relates to IT security.

Cyber security [15, 35]is the newest variant of security. The word cyber has become very popular, although there is no clear definition of it. Mostly it is defined as a prefix that is "relating to computers and the internet" [49]. Cyber security has become a matter of national security since the late 2000s [69]. Just a few documents distinguish between cyber and information security. Therefore it can be assumed that in most cases when experiencing a cyber security incident, there was a loss of confidentiality, integrity, and/or availability. One difference is that in cyber security it is not relevant if you or another system has lost their CIA. Another difference is that information security addresses people as a risk factor which needs to be mitigated through training to secure information, while cyber security sees people as a resource worth protecting. Cyber security addresses information and IT as the vulnerabilities. Indeed, a characteristic of cyber security is the fact, that all assets worth protecting need protection because of the use of IT systems. Cyber security can be seen as an extension of information security. Four scenarios have been described that extend cyber security to people; bullying, (home) automation, media, and terrorism. Cyber bullying means the massive bullying of people over the internet. The automation scenario indicates expansion of the meaning of security to safety aspects as well. Stuxnet may be seen as the first state-sponsored cyber attack [46]. The media scenario is described by financially hurting the stakeholders of information when illegally downloading and sharing it [69]. Due to the recent activities of fake news and facts, the rise of fake information in digital media and its outcome like damaging social structures of any kinds should also be considered [60]. Last but not least, the cyber terrorism scenario depicts the manipulation or severe damaging of

critical infrastructure (power, water, health, finance, etc.) to damage society or a nation and wage war onto them [69]. This leverages cyber security into an ethical dimension whether or not to attack a system. Cyber security aims to protect the trust a society lays into an IT system [40]. All definitions address the core parts of the CIA triad, con-

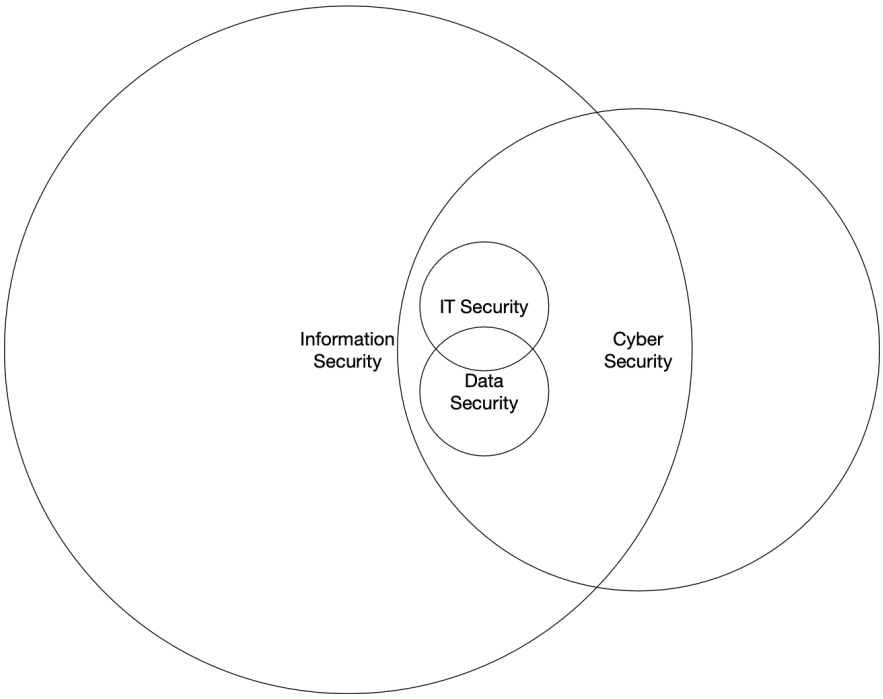

Figure 2.1: IT security and data security are different fields, that strongly depend on each other. IT security is about IT systems, while data security is about data stored on IT systems. Information security fully implements IT and data security and extends it to information stored on IT systems as well as on paper and memorised by people. Cyber security even extends information security as it utilises the core principles of information security (CIA) and adds people and society as an asset worth protecting.

fidentiality, integrity, and availability. Security means to protect assets from all forms of threats and vulnerabilities [69]. It does this by implementing security controls to reduce the risk of identified vulnerabilities. Information security addresses all information, while IT security addresses information stored and processed on IT systems, as well as the corresponding processes. IT security never addresses information alone, while information security also addresses non-IT processes. IT security attempts to protect IT systems, while information security attempts to protect information itself.

Data security solely focuses on securing the data itself, therefore, access to and from data and how to properly store it. Data security is a big part of IT security, while IT security plays a role in information security. Cyber security ranges from protecting people or society, to household appliances and industry machines, as well as national or international critical infrastructure. “In fact, such assets include absolutely anyone or anything that can be reached via cyberspace” [69]. A visualisation of all four definitions and their influence is pictured in Figure 2.1.

2.1.3 Safety and Security

As already described, in an IT and OT context, safety protects life itself from machinery, while security protects objects from other objects and life. Of all the mentioned variants of security, only cybersecurity addresses safety aspects. Safety is dependent of security but not vice versa. Therefore, safety measurements are affected by security measurements and missing security measurements, while safety measurements themselves have no impact on security. An example: Missing permissions may affect controls for an industry robot, which may go rogue, while a rogue robot has no affect on the permission settings. Nevertheless safety needs to be achieved. Good security is a key to reach this goal.

2.1.4 Data Protection, Privacy

Data protection and privacy are related terms but have a different meaning in detail.

Data protection is a term for securing data in a regulated way. Therefore, there are laws (e.g., GDPR) that regulate the measurements that need to be applied to specific kinds of data. In terms of GDPR, that means, for example, only gather the absolute least amount of Personal Identifiable Information (PII) that is required to provide a service [18].

Privacy is to be seen more as a right and/or a concept to have the sovereignty of own data [58]. Privacy is a part of data protection and needs to be considered to accomplish it and be compliant [18] but the exact peculiarity of the privacy concept differs by culture and society [58]. Privacy is also defined as "the quality or state of being apart from company or observation" and the "freedom from unauthorized intrusion" [53]. Privacy is a concept that applies to data of people and organisations!

2.1.5 Information Security Policy and familiar terms

When addressing policies, directives, and guidelines, this thesis means its normative sense as described in the first two paragraph of this subsection, if not marked any further.

A *policy*, as defined by the ISO 27000, is described as "intentions and direction of an organization [...] as formally expressed by its top management" [25]. A policy is therefore a document that is approved by the top management [25, 26] and all other internal regulations need to subordinate to the policy, therefore they need to comply to the policy. The governance of an organisation need to assure that a policy complies to external regulations (e.g.: laws, contracts, certified standards, etc.).

Guidelines or *guides*, or *directives* as named at the ISO "are documents that provide advice [...] on how to deal with specific issues when drafting standards" or "on how to deal with issues specific to standardization principles" [31]. A guideline is to be seen as help when creating standards or policies and may be of help when implementing a policy [30].

Regulations are European laws and "have general application, are binding in their entirety and are directly applicable in all European Union (EU) Member States" [20]. That means, this law is applicable and directly binding and there is no interaction of the member states required. Also, similar to directives, a national law cannot outlaw a

European regulation.

A *directive* as in the meaning of the European Union "is a legal act adopted by the EU institutions addressed to the EU Member States and [...] is binding as to the result to be achieved" [17]. Therefore, on the contrary to regulations, it means that the underlying law primarily needs to be transformed by the member states into national law to become applicable law. Directives declare where member states need to fully copy regulations from the directive into national law, and where member states are allowed to differ within a range (e.g.: the age limit for youth protection and, therefore, directives relating to youth protection mostly allow member states to differ the age limit.)

An *Information Security Policy* is a document, that governs processes and the actions of personnel in relation to a specific topic and is derived from an *information security guideline*. The information security guideline is, on the contrary to the guideline definition of the ISO, the top level document in an organisation of the information security management which is signed and approved by the top management. The information security policy describes the a specific process of the organisation in terms of information security. It also serves as an internal regulation for personnel about certain processes and allows and/or forbids certain actions. The information security guideline describes the intentions of the information security management of the organisation and its goals, while the information security policies describe specific actions based on the information security guideline. Therefore, ideally, an organisation has one information security guideline and multiple information security policies. Figure 2.2 visualises the relations of the various documents.

Information Security Management or *Information Security Management System (ISMS)* is the term to describe the comprehensive approach of an organisation to information security. An information security guideline and its derived information security policies are a part of it [26]. An organisation "shall establish, implement, maintain and continually improve" [26] its ISMS to create a working and standardised compliant system.

2.1.6 Risk, Threat, Vulnerability

A *vulnerability* is described as "intrinsic properties of something resulting in susceptibility to a risk source [...] that can lead to an event with a consequence" [32]. A vulnerability is a property that exposes a software, process, or entire organisation to a threat. It is the error in the action. A *threat* is a negative event that takes advantage of a vulnerability. A *risk* is an "effect of uncertainty on objectives" [32]. A risk may be described as the possible damage done through a threat in combination with its probability of occurrence.

To explain this with a real-world example: A vulnerability in MS Exchange was found (CVE-2021-26855[2]). A group called Hafnium created a threat by exploiting this vulnerability. In this scenario, Hafnium was the threat actor. The risk would be the possibility of successful exploitation of this vulnerability in an organisation through this threat and its possible damage. Possible questions to ask when evaluating the risk: Is MS Exchange being used in this organisation or in corresponding other organisations? Are there any mitigation measurements in place (a patch, a firewall, an Extended detection

[2] https://nvd.nist.gov/vuln/detail/CVE-2021-26855

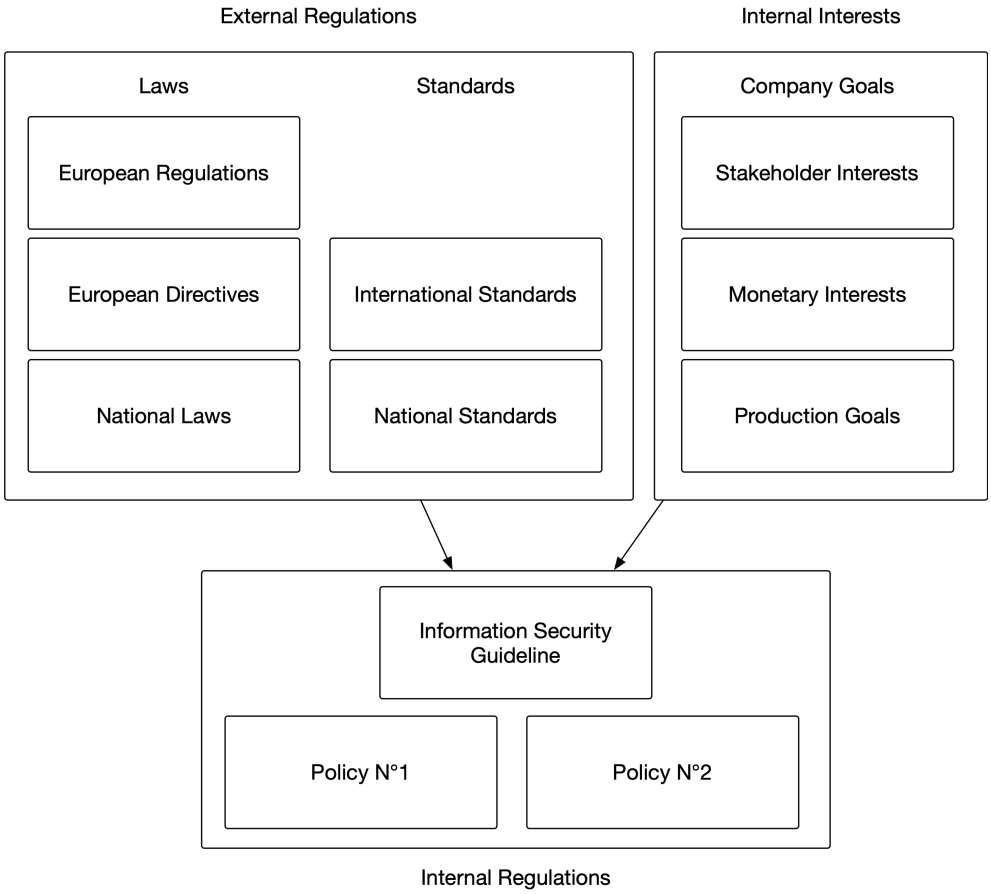

Figure 2.2: External regulations, consisting of laws and standards, and internal interests are used to derive internal regulations. Union wide law weights more than nation wide law, but law always weights more than standards or internal interests when creating internal regulations. The internal regulations rely on a top level document; the information security guideline. From this guideline, multiple policies are derived.

and response (XDR), etc.)? Is it a critical system? What is my possible damage (CIA, money, reputation, etc.)?

An information security policy "can only maintain risk, whereas compliance with the information security policy can modify risk" [34], which means that a policy on a piece of paper does not mitigate risk, but compliance with the policy, therefore trying to apply measurements derived from the policy, does modify and therefore may mitigate risk, if the policy has a correct understanding of the risks.

2.2 Basics of Risk Management

Risk management is all about identification, evaluation and prioritisation of risks. There are various international standards that describe a standard procedure about it (e.g.: ISO 31000 [28] is about general risk management and ISO 27005 [27] is about risk

management specific to information security; BSI 200-3 [21] is about risk management specific to IT operations written by the German government). *Risk management* is a term for the "coordinated activities to direct and control an organization with regard to risk" [32]. A *risk management framework* is "a set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring [...], reviewing and continually improving risk management [...] throughout the organization" [32]. The ISO 31000 defines risk management as "an integral part of all organizational processes" and a "part of decision making" which "creates and protects value" [28]. To get a working risk management, the organisation management should commit itself to a risk management policy.

2.2.1 Risk Processing

A risk needs processing in its life cycle, meaning it needs to be treated in a specific way starting from its identification to its eradication. The following paragraphs explain the different steps and when to apply them [28]. Figure 2.3 visualises the steps for a better understanding.

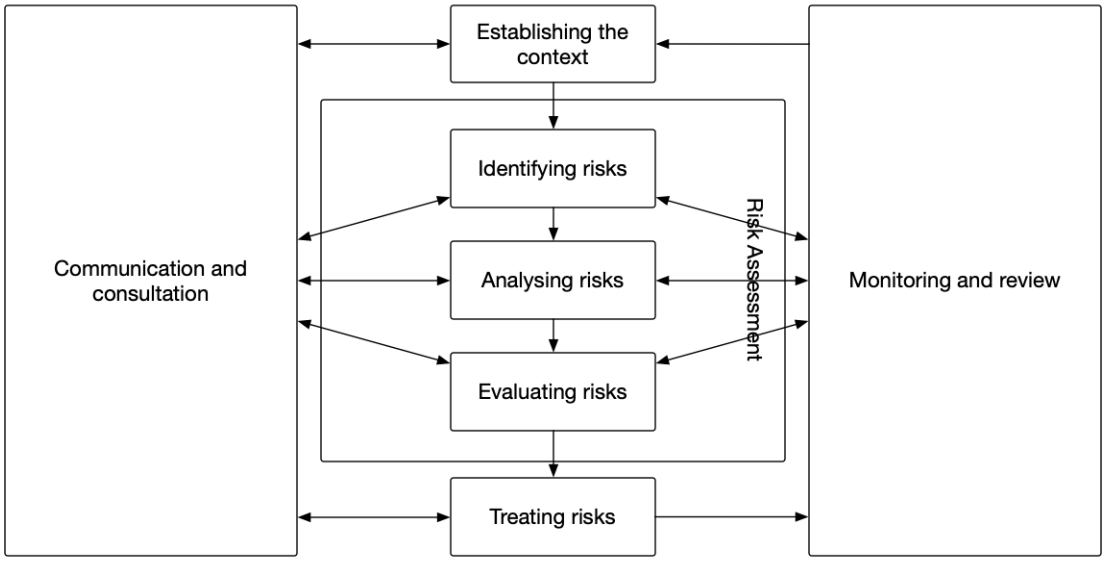

Figure 2.3: Risk management is a process/cycle [28]. It starts with establishing the context going to the risk assessment (including identifying, analysing, and evaluating risk) and treating risks followed. Monitoring and reviewing follows treating risks and starts the cycle again (cf. Plan-Do-Check-Act (PDCA) cycle [37]). During the risk assessment there is also a constant monitoring and reviewing. Also during all steps, communication with all stakeholders and getting/giving consultation is a crucial step.

The first step is to *establish the context* of the system. Understanding the system, its needs, and its context for the organisation is crucial for the entire following steps.

The next step is the *identification* of a risk. To identify a risk a certain knowledge of the system and a certain awareness of risk is required. The more knowledge of a system and/or the more aware people are about a system, the more sophisticated risks might be

identified. Not identifying a risk does not mean that the risk does not exist! Risks should be split into "known known" and "known unknown" risks. Also, one should always be aware that there are "unknown unknown" risks.

When a risk is identified, there is a need for risk *analysis*. When analysing risk, there is a focus on the causes and consequences of the risk, as well as an analysing of the likelihood of its occurrence. Common analysing methods in software development are STRIDE [78] and DREAD [62].

The last step of risk assessment (cf. Figure 2.3) is risk *evaluation*. The evaluation prioritieses risks and their treatment based on this analysis. A comprehensive analysis is crucial for the evaluation process.

A milestone in risk management is the risk *treatment*. Risk treatment needs to find a balance between the possible risk damage and occurrence, and the costs of the risk treatment. Treating risks may have the purpose to reduce the risk, to sell the risk (e.g. an insurance), or to simply accept the risk. Reducing the risk might reduce damage and the likelihood of occurrence, selling the risk only reduces damage but not the likelihood of occurrence, while accepting the risk does not manipulate the risk at all.

Monitoring and review is the name of last step in a risk management process and the step to restart the circle. After the risk treatment, the risk is monitored and the measurement are reviewed about their effectiveness. Monitoring and reviewing the intermediate step during the risk assessment should also happen.

Communication and consultation is an ongoing process parallel to all other steps. During the cycle it is necessary to inform stakeholders about risks and to consult them about the risks. Also, it might be a good idea to get some consulting while managing the risks.

2.2.2 Roles of Risk Management

Risk management is a process affecting the whole organisation. Therefore, there are multiple roles to handle risk management. Some roles must be assigned to different people while other roles may be assigned to the same person. The terms "accountable", "responsible", "consulted", and "informed" align with the RACI-chart [65].

The *risk owner* is the role which is accountable for a specific risk. The risk owners may align with product owners or other roles (e.g. data protection officer as risk owner for data protection relevant risks). The risk owner is accountable for managing the assigned risks and is encouraged to consult the risk manager when deciding treatment.

The *risk manager* is responsible to work on the risk management cycle. The risk manager does most of the tasks in the risk processing (see subsection 2.2.1) except decision making. Decisions are made by the risk owner.

The *risk management framework owner* is accountable to develop, maintain, and implement the risk management framework.

The *user* is the role working with the tools and processes where risks arises. Therefore, users are either the cause and/or affected by the risks. This means they need to be informed about risks to avoid causing them or avoid being affected by them.

It is a good idea to separate the risk management framework owner from the risk manager. The risk owner might be the risk manager. The role risk manager is recommended to be fulfilled in a full time employment while risk owner and risk management

framework owner can probably be assigned to people with other non-risk-related roles. The user might (and probably will) be combined with any other role.

2.3 Basics of IT operations and service quality

IT operations is a set of IT services and processes that a group of dedicated people (IT professionals) provide to internal and external customers as well as themselves. These people may be organised in various ways; including departments, IT professionals assigned to various specialised departments, and external organisations. IT operations strongly rely on policy sets, defined responsibilities, and a portfolio management (what service is provided to whom). To achieve a set of quality, quality management should be applied (cf. ISO 9001 [29]).

The standard guidelines about IT service operation and IT service quality assurance are *Information Technology Infrastructure Library (ITIL)* [73] and *Control Objectives for Information and Related Technologies (COBIT)* [75]. The following subsections describe these standards. They describe IT operations as a service which is delivered to the customer. IT service management strongly focuses on the needs of the customers and should be improved continuously.

2.3.1 ITIL

ITIL focuses on IT service management and IT asset management. IT management has the goal to implement existing policies in order to provide efficient service to any sort of customer. It is a framework developed by the british government in the 1980s to standardise IT service management across the governmental IT service providers. Since then, it has developed to be a standard owned by a private company which organisations can still certify to. It is one of the most widely used frameworks for IT service management [48], as it standardises the selection, planning, delivery, and support of all of the organisation's IT services. In its current version (version 4), ITIL provides a significantly higher amount of guidelines, such as architecture, organisational change, and project management [24]. It comes with seven guideline principles: "Focus on value, Start where you are, Progress iteratively with feedback, Collaborate and promote visibility, Think and work holistically, Keep it simple and practical, Optimize and automate" [24].

2.3.2 COBIT

COBIT is a framework about IT governance. Governance focuses on creating policies that align international and national law and consider an organisation's interests (see Figure 2.2). A part of governance is also responsible for verifying compliance of managements implementation of the given policies, therefore, auditing the organisations IT system. COBIT consists of five components which are described below:

- *Framework*: COBIT is a framework to organise objectives and best practices about processes and organisation requirements.
- *Control objectives*: It provides a complete set of control objectives to effectively control IT processes.

- *Process descriptions*: COBIT provides a reference process model to map responsibilities of the processes to the PDCA cycle.
- *Management guidelines*: The governance framework supports the assignment of responsibilities, measurement of performance, agreeing on objectives, and illustrates the relationships between processes. This helps in getting a better understanding of the overall liaison of processes and business units.
- *Maturity models*: COBIT assesses maturities and capabilities of the processes and the teamwork of the units.

These components are aligned with ITIL and Capability Maturity Model Integration (CMMI), and also is capable to integrate the ISO 27000 family. The CMMI (see Figure 2.4) tries to measure the maturity of a process and categorises it into one of five stages. This categorisation helps identifing a need of improvement of various processes. COBIT aims to maintain independence from specific manufacturers, giving a framework applicable to all technologies and platforms.

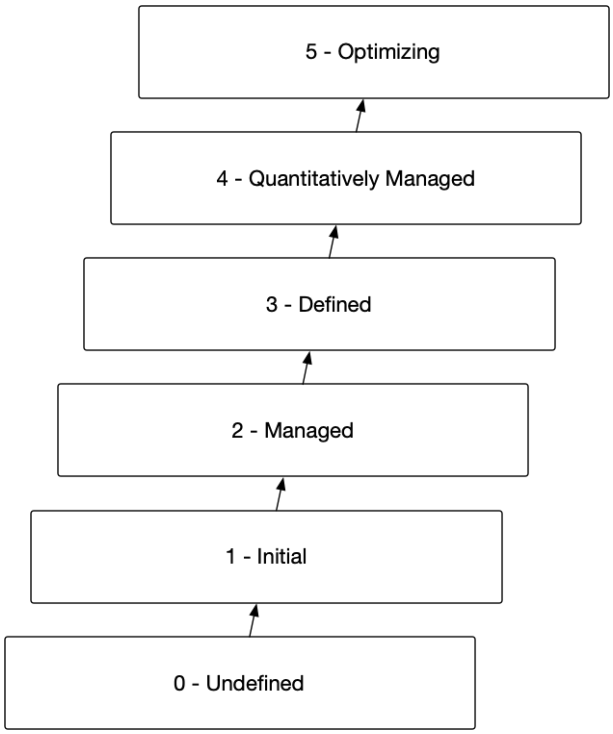

Figure 2.4: The CMMI tries to define state of maturity for processes [74]. The higher the number of the maturity rating per process, the more mature it is. Organisations strive to achieve a high maturity per process.

Chapter 3

Related Work

Finding related work to this topic is a quite difficult task. Most of the work done relates to merging technical policies and focuses on the technical approach to do so. Other publications are vastly outdated.

A promising publication is about merging technical security policies (access controls and permission sets) [4]. The author tried to merge varying security policies of an Organization-Based Access Control (OrBAC) and proposes a strategy to resolves conflicts when merging them. The author states that there might be problems when inheriting permissions and access controls, where conflicting statements will be defined. To solve this problem, the priorities in the statements defined and the specificness of objects and areas of impact need to be taken in consideration. This work solely considers technical problems with permission heritage in technical security policies.

Another publication is in fact about merging security polices [41]. The authors tried to merge policies of a parent and subsidiary company. The paper focuses on an assurance case only, and describes the merger of a policy while the authors do "interviews to three experts in information security". Apparently, the methods of this paper were quite specific for the described problem. Therefore, the results are not applicable to this thesis.

A clinical decision and alert system was designed with parameters of mindspace [23]. The authors of this paper reviewed over 1000 studies between the years 1970 and 2022 and analysed them regarding the mindspace parameters and effects. The authors argue, that mindspace has already been widely adopted in healthcare and surrounding areas including their decision making systems. The questions of their work were:

- "[...] how can mindspace effects inform alert and reminder designs?"
- "[...] how effectively can they influence clinical decisions?"

They were able to improve performance of these systems significantly when designing them with mindspace, than with no behavioural forming framework. Another mindspace related work was about nudging health promotions during the COVID-19 pandemic [64].

Mindspace is a great tool for communicating and helps in transporting the relevant parts of a message to the relevant receipients. It has been widely used in health care and proved its effectiveness there and will be used in this thesis as well. As written later on, mindspace will be a key framework in trying to achieve the research goals. It is believed that the communication principles of health care could be applied in cyber security also.

Chapter 4

Hypothesis and Theory

A security policy framework consists of multiple policies guiding and controlling workforce into a desired behaviour. This thesis is about merging two entire policy frameworks into one. Each policy and policy framework has been assigned a specific, different scope. This thesis proceeds on the assumption, that the scopes of these policy frameworks dissolved and, therefore, there is a need to consolidate the policy frameworks and all its policies. This thesis tries to find an ideal communication scheme using already known and defined frameworks to notify and educate all stakeholders about policy changes to correctly comply to policies.

4.1 Theory

A successful merger of security policy frameworks and a successful notification and education needs to address all stakeholders of these policy frameworks. These stakeholders are as follows:

- employees, who are adressed by the policies
- executive management, who is responsible for the compliance of the company and its doings
- external regulatories, such as legislative, law enforcement, and an auditor of a standardisation organisation

There should be a balance between understanding the content and the importance of specific stakeholders to the functioning of a security policy. If the content and/or the importance of a relevant policy is not understood and not implemented by one of these stakeholders, the overall security of the organisation is weakened. Also, there is a difference between the importance of different people understanding the policy. The regulatories and management are multipliers to policy understanding and implementation. If the regulatories do not understand the importance or content of a policy, it may never be implemented in any organisation. If the management may not understand the topic, it will never be implemented in the reach of the mangement, therefore in (parts of) the organisation. If employees do not understand the policy, it may never be executed by the employee, but, nevertheless, the employee needs to comply its doings to the policy. All of these lacks of understanding result in a vulnerability of the organisation which leads to a risk (see subsection 2.1.6).

It is strongly believed, that people need to be aware of security and its problems, including the part that people themselves have in security. Therefore, the following hypothesis - to create a successful merger of both policies and to satisfy all stakeholders - is strongly based on the following two principles; the security awareness cycle and the influencing of behaviour of the framework "mindspace". Both principles are quite easy to understand, seem to be applicable, and are easy to access. Also, *mindspace* is quite popular in literature (see chapter 3). The security awareness cycle will be used as a framework to manage the change it self, while mindspace will be used to communicate it to the stakeholders. These principles will be described in the following paragraphs. Mindspace is the key principle of this thesis. The thesis tries to vary different parameters to get to an optimal notification scheme and educate people about the changed policies. Also, it is a key to the thesis to get people to comply to the policy, which is a part that should be achieved with mindspace. Mindspace has been widely in use in other scientific fields. It seems to be conclusively and is therefore used in information security as well.

4.1.1 Security Awareness Cycle

The security awareness cycle is a framework to create and/or increase security awareness to people [77]. It is based on six steps:

1. *Security Awareness Metrics* - Collect metrics to measure the process. These metrics are used to get an understanding of the quality of the process and help identify fields where adjustments are required. The metrics need to be defined based on the field of research.
2. *Identify and Understand your Audience* - Identify the various audience groups in your organisation. Distinguish between roles and risk profiles of your audience and also evaluate the already present awareness and skillset, respectively the missing awareness and skillset.
3. *Identify High-Risk and Desired Behaviours* - Get an understanding of the various behaviour, especially the high-risk behaviour of your audience. This behaviour may correlate with the skillset of the audience.
4. *Identify Solutions to Faciliate Behavioural Change* - Decide on how to handle the behavioural change. Create one or multiple solutions to focus on.
5. *Create Security Awareness Materials* - Create material to support the process of behavioural change. These materials may include email templates, presentations, movies, posters, etc. This material should be memorable. It is also advised to create the material without the use of classified information, to encourage people to spread the word and share the material.
6. *Deliver the Message* - The last step is to deliver the message. The message should focus on the solution of the fourth point and use materials of point five. This is the step, where information and manuals to change the behaviour is brought to the audience.

This six step guideline should be used to eliminiate the most risky behaviour. Also, as visualised in Figure 4.1, these steps could be used in an adapted PDCA cycle. Therefore, in each cycle the current most risky behaviour is addressed, and the risky behaviours are eliminated step by step. The security awareness cycle has a very low citation rate,

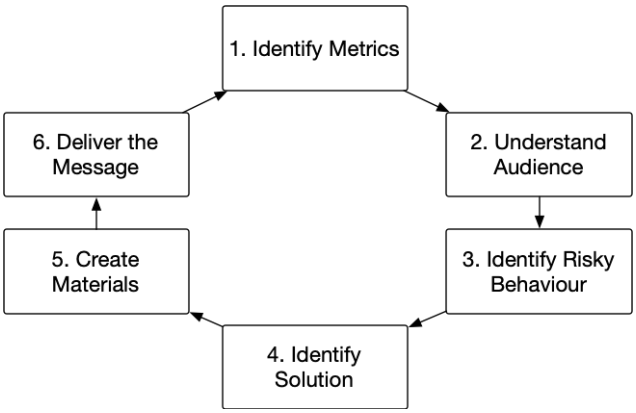

Figure 4.1: The Security Awareness Cycle tries to change risky behaviour of humans [77]. It can be regarded as a PDCA cycle to address the most risky behaviour per cycle.

but adapts the already known PDCA to cyber security. It creates an easy to understand management cycle to improve awareness programs in organisations, and therefore, raise awareness itself.

4.1.2 Influencing behaviour

Mindspace is a framework to subtle adjust behaviour of people and could therefore also influence acceptance of change [12]. It defines nine "effects" to influence behaviour which will be shortly described below:

- *Messenger* - "We are heavily influenced by who communicates information to us" It is important to choose the right messenger. People tend to comply to messages of authorities. Also, messages of people of the same circle of interests are more likely to be seen trustworthy and have a high chance to act persuasive. There is evidence, that we as people associate a feeling to the messages of the messenger which affects the trustworthiness of the message and therefore the willingness to comply with it [14].
- *Norms* - "Our responses to incentives are shaped by predictable mental shortcuts such as strongly avoiding losses" - Social norms shape our behaviour. "[...] individuals take their cues from what others do" [12].
- *Incentives* - "We are strongly influenced by what others do" We are people with an economical understanding. We are aware of the prices of our doings and thrive for an incentive as a reward. Giving incentives to change behaviour improves the results. Nevertheless, incentives depend on other factors such as type, magnitude and timing.
- *Defaults* - "We 'go with the flow' of pre-set options" When people do not have knowledge and/or an opinion about a topic, they usually choose the default option. Also, choosing the default option creates the illusion of not having to decide.
- *Salience* - "Our attention is drawn to what is novel and seems relevant to us" Our behaviour is influenced by our attention. People tend to register novel, accessible, simple, and apparently relevant events.

- *Priming* - "Our acts are often influenced by sub-conscious cues" When behaviour should be influenced, exposing certain words and sights beforehand is desired. People tend to act more influential to information that the have already heard of.
- *Affect* - "Our emotional associations can powerfully shape our actions" Emotions are influencial in our behaviour. Assigning positive emotions to a desired behaviour improves behavioural change enourmous.
- *Commitments* - "We seek to be consistent with our public promises, and reciprocate acts" People tend to procrastinate and delay decisions. Creating public available commitments help people to meet desired goals and deadlines.
- *Ego* - "We act in ways that make us feel better about ourselves" People see themselves in a self positive way. Creating competition may increase the adaption to a desired behaviour.

Table 4.1 summarises the model.

Mindspace is regarded as a nudging method. Nudging has been met with enthusiasm, while also being heavily critised ethically. "Nudge policies try to improve people's decisions by changing the ways options are presented to them, rather than changing the options themselves or incentivizing or coercing people" [61]. Nudging should only be used in ethically unproblematic situations.

Messenger	The person transporting the message and the related properties: authority, friendship, specialist, etc.
Norms	Which culture does affect the receipient?
Incentives	What is the profit of the receipient when doing the recommendations of the message?
Defaults	The default options are the ones that most people pick
Salience	People are interested into novel and easy to understand things.
Priming	Formulate the message accoring to the education level of people.
Affect	People will assign an emotion to the message.
Commitments	We do what we commit ourselves in public.
Ego	We try to improve our ego.

Table 4.1: Mindspace Parameters that influence behaviour of other people. If adjusting them when communicating a message, the resulting behaviour of the receipient is changed [12].

4.2 Audience-Aware Language

The message, that addresses an audience, needs to be adapted depending on the audience. To address an audience perfectly, a message must match the motivation of the audience and the cognitive abilities. Matching the correct motivation is a key to get

someones interest. If people are not interested into something, things mostly aren't learned or done in a high quality.

Also, if not using the correct language regarding cognitive abilities, people will lose interest. In fact, if an incorrect language is used, people may feel disturbed and unappreciated. Loosing interest leads to the consequences mentioned above. Furthermore, not using the correct language leads to people not understanding the message. This is also an important factor, as not understood messages cannot be complied to.

4.3 Possible Metrics

To formulate a possible theory, metrics need to be defined. These metrics or Key Process Indicator (KPI)s are needed to measure, if the chosen process method improves the performance of the policy, or if the merger of the policy framework was successful at all. The following metrics will be measured. These metrics have been defined as part of this thesis.

- *Policy Redundancy* - How many policies or parts of policies are defined redundantly?
- *Comprehensability* - How many questions are being asked by employees about the policy?
- *Maintainability* - How much time is needed to maintain the policy?
- *Implementability and Applicability* - How many policy violations have been reported or observed? How intense have been these violations?
- *Incidents* - How many security incidents have occurred? Incidents may be a indicator of a policy violation but it is not necessarily. An incident is an event, where the security of the organisation, information and/or data has been compromised.
- *Recommandation* - Is this approach worth a recommendation?
- *Improvement* - What aspects of the approach could be improved in another cycle?
- *Understanding* - Employees will get questioned, if the new policy is more understandable than the previous one?

These metrics are to be measured in defined time frames. These metrics serve as indicators of success to different methods. Therefore, the performances of the different issues as performed in section 5.2 are compared with these metrics.

The chosen theory to tackle the change of the policy framework and to successfully notify and educate people about the changes is to combine the principles (security awareness cycle in subsection 4.1.1 and mindspace in subsection 4.1.2) described in the sections above.

The policies should be merged one by one for two reasons. First, the stakeholders have time to understand the change and implement it. Second, the change process can be monitored and adapted if needed, accoring to a PDCA-cycle (see subsection 4.1.1). Also, according to the security awareness cycle, the most critical policy, where the highest security risk should be tackled first, followed by the second highest security risk, and so on. The higher the risk, the sooner it should get handled.

After changing a policy, people need to get notified and educated, which is where the principles of *mindspace* need to be used. The identified audiences need to be addressed

particularily. The mindspace parameters differ per audience and objective. The objective stays the same (a policy gets changed, employees need to comply to it), but the audience differs. The organisation itself stays the same, but inside the organisation, there are different audiences. In this thesis, some influencual effects of mindspace may stay the same as the objective stays the same, some need to differ per audience. These parameters will be shown in the following list:

- Messenger - A matching messenger needs to be found for every distinguished audience. Every audience acts different about authorities, therefore, a matching level of authority needs to be found.
- Norms - Norms may be found for every distinguished audience. As norms are a social influencial effect, the same findings will probably match for the entire audience, if it is in a small company. This differs a lot, if multinational organisations are addressed.
- Incentives - Appropriate incentives need to be developped per different audience. There may be a unified incentive, but an individual incentive per audience is much more efficient as it better meets the motivations of the respective audicence.
- Defaults - As already described, people tend to select default settings. There is no need to create multiple default settings per audience. The desired results of all audiences are the same, so the default may be the same to all audiences.
- Salience - Novel, relevant topics need to be identified per identified audience. In a typical organisation, people work in all sorts of discipline. People not working in IT, even people working in IT, have a different experience with news and know something different about the same topic. Specific news is only memorised by specific people.
- Priming - Explaining the reasons of a policy shift is essential to get the understanding of people to comply to the policy and to actually give constructive feedback about it. The reasons do not have the need to differ.
- Affect - Every audience group has different emotional bindings and motivations, therefore, different emotional associations need to be created.
- Commitments - There could be two commitments. An organisation wide one and one per smaller audience. The organisation wide commitment will drain less resources in creating an maintaining it, but will also generate less effectiveness than an individual one.
- Ego - To address the ego parameter, the message could be turned into a challenge. This challenge may be an organisation wide contest comparing departments or individuals. This results in a unified ego per organisation.

These described effects and the resulting measurements created for the case study and furthermore for the later implementations need to be scaled to the organisation. Also, the existing audiences need to be evaluated to their usefulness and efficiency to the case study. Surveying for available audiences may result in an enourmous number, which cannot get served. The final, resulting subset of addressed audiences need to be a subset of the original number of audiences, that could be maintained and worked with. Merging audiences, that only differ in a nuance is advised.

The resulting policy needs to be published via an available method which is accessible

to the required audience. The method should be able to respect the CIA-triad. Therefore, it should support permissions (e.g. there may exist sensitive policies) - confidentiality, and automatic versioning - integrity. Versioning is needed for two main reasons:

1. Policies must not change without notice. Any change in a policy needs to be visible and if a change is made, stakeholders should be notified.
2. Policy changes should be easily comprehensible. A summary of the change (e.g.: an automatic generated diff) may support stakeholders in understanding the policy, especially the new version. This may be done in a way, similar to *Redline* from the ISO [76]. All changes are marked in an understandable way, differenciating between new information, deleted information, and changed information.

Achieving versioning with a technical approach is highly recommended.

4.4 Hypothesis

The hypothesis describes the approach that is believed to be the most efficient one in merging information security policies and, therefore, notifying and educating people about the change. The approach of the hypothesis is as follows:

1. Policies are published via a tool that supports versioning. This tool is able to record every change and is able to compare different versions (e.g.: *git*, *wiki*-style tools, etc.). Also, the user and reader of the policies is able to use these features.
2. Policies are published via a tool that supports a subscription to automatic change notifications. Users are able to subscribe to policies or group of policies and are notified automatically about changes. Configuring the granularity of notifications is possible.
3. The messenger is the manager of the respective department of the organisation. The manager has the correct amount of authority to enforce changes combined with the correct amount of affiliation to the respective teams. Also, the approach scales to any form of organisation in terms of time resources of people.
4. Encourage a “try out new things” norm, but also address an “it has always been that way” one. This encourages the wanted culture to embrace itself but also tries to fetch employees of the unwanted culture and may nudge them to join the “try out new things” culture.
5. Offer a positive incentive. A positive incentive, therefore, something that someone can gain is a stronger motivation than a ban and restraint of something.
6. The policy is written in a default way, therefore, the existing workflow and defaults are considered and implemented into the policy. If the policy needs to be different to existing workflows, technical enforcements are in place to support employees to comply to the policy where possible.
7. Subscribers of policies are notified about all changes of the policies (respectively on their configured granularity). Nevertheless, relevant employees are always notified (and educated) about relevant changes via their messenger, therefore the manager of the respective department.
8. Focus communication about policy changes to already established employees. They may have internalised the old policy which needs to be changed. New employees

should get educated about policies during their onboarding phase.

9. Create a happy emotion about the policy change. Embrace people and their doings, respectively importance of themselves and their doings.
10. Let people commit in the organisation to the implementation of the new policy. Create that commitment in a self-reminding way.
11. Communicate the changes that people may boost their egos, when implementing the change.

The items above are numerated for marking purposes only (e.g. section 5.5), and are not weighted in any kind. The following case study and its different issues try to validate the hypothesis.

Chapter 5

Case Study and Analysis

This chapter describes a case study carried out in an organisation. It describes the initial situation, including details about the organisation. Next, the design of the various issues are described which are carried out, followed by the gathered metrics, and an analysis of the metrics.

5.1 Initial Situation

The initial situation, that this thesis tries to analyse and solve is the following: An organisation has two separate, different security policy frameworks. These policy frameworks define accountability, operations, service, etc. for two separate business divisions, also considering the overall knowledge and ability of users to operate an IT system. Therefore, there is no and has not been any interaction between these divisions. The organisation has around 200 employees, 50 of them are using IT devices regularily. It is located in Austria, and is considered critical infrastructure with a highly valuable set of data. The employees are aware of the value of the processed data. The case study covers the entire organisation but focuses on the employees that regularily use IT-devices.

These division are to be merged, including their policy framework. As the scope of the previous security policy frameworks dissappeared, there is an immediate need for a merged security policy framework. The problems that arise, including the difficulty to train users and administrators, completeness of the asset inventory and necessary information, and identifying blind spots are subject of analysis and possible solutions are being proposed.

The following subsections will summarise the content of the different policy frameworks. We will refer to them in this thesis as policy framework A and policy framework B and are described in subsections below.

5.1.1 User Groups

This thesis defines and differentiates between three user groups:

- Power users are defined as users that have a good overall knowledge about IT and their operations, they know their own discipline, they are able to help themselves, and know on how to read and interpret a policy.

- Standard users have a very basic knowledge about IT. They know their own discipline but need a lot of help when operating a new software, and don't know how to read and interpret a policy.
- Administrators are IT administrators who have an excellent knowledge about IT and their operations (which is their business). They are able to help themselves, and are able reading and interpreting a policy, including creating one.

The organisation, which resulted after the merger, consists of approximately the same amount of power users and standard users among all employees that use IT assets. Administrators represent a minority in the organisations workforce.

5.1.2 Summary: Policy Framework A

Policy framework A is applied to division A. Division A has a few standard users, a majority of power users, and some administrators. Policy framework A is very user friendly, as it allows users to install software on their own, but they are also responsible for their own IT-devices. All risk assessments and evaluations of software, that is installed by the user, are delegated to the user. There are data classifications, which need to be applied by the user themselves. Users need to decide, which data is classified in which category and if a software is allowed to process this kind of data. Also, the policies are published via a searchable documentation management system, which supports an easy to define permission set by the information owner, automatic versioning including notifying stakeholders and summarising diffs. Policy framework A might be summarised as:

- Decide yourself which software to use, simply commit to this framework.
- Decide yourself on how to classify data, simply commit to this framework.
- You are responsible for the information and device.
- The organisation believes you are capable of making good decisions about information.
- The policies are published via a searchable documentation management system.

This sort of policy framework requires low technical enforcement and surveillance, as it is assumed the user is able to decide, what is best for the organisation. This sort of policy framework requires highly trained and trusted personnel.

5.1.3 Summary: Policy Framework B

Policy framework B is applied to division B. Division B has a majority of standard users, very few power users, and a few administrators. Policy framework B is more restrictive than policy A. It does not allow any software installation by users. Every software and/or significant change on an IT system needs the approval of an administrator. Risk assessments and software evaluations responsibilities are devided between the users and the administrators with a strong focus on administrators. Permissions and access are granted on a least privilege principle. These policies are published via a fileserver. Policies are organised in folders, which try to represent the organisations structure, but does not fully achieve this. Searching is supported as the fileserver supports it, there is

no versioning and no change notification; file permissions can only be changed by the fileserver administrator. Policy framework B might be summarised as:

- We deliver every software you need, you have no freedom to choose.
- Work with the tools that we provide.
- You are only partly responsible for the information and devices.
- The organisation does not believe that you are not capable of making good decisions about information.
- These policies are published via a fileserver.

This sort of policy framework needs a lot of technical enforcement and surveillance, it needs a lot of organisational work, but does not require highly skilled personel.

5.2 Case Study Design

Multiple case studies have been carried out using the theory and initial situation described above.

The case study tried to comprehensively merge two policies into one, satisfy all stakeholders to a possible maximum, and publish it regarding the CIA-triad. This case study has been done in various tries (termed *issues* later on). The observed timeframe of the case study is six months per issue. This means, the observed timeframe starts at the time of publishing the new policy and ends six months afterwards. As the different policies vary in their publishing date, the end date of the observation also varies. The years of observation were 2023 and 2024.

As the divisions were merged, there has not been a clear cut in the workflows, old structures and mindsets kept on existing. The described issues below have been designed and executed by different people coming from different divisions and, therefore, different workflows. One person was from division A, another one from division B, and another one has been hired after the merger. Therefore, the person from division A created policy mergers using old structures of division A, while the person from B does it via structures from B. The new person works with a hybrid structure. The following issue 1 has been created by the person of division B, issue 2 by the person of division A, and issue 3 by the person hired after the merger. The numbering of the issues and the naming of the divisions do not correlate. Therefore, people still use their historical communication channels to notify about changes, although they increased their scope of policy creation and education of changes from their division to the entire organisation. Finding this occurence was part of creating these issues and are already empirical research. Comparing the different approaches and structures, respectively finding already good working parts and parts in need of improvement, is a goal of this thesis.

A new information security guideline (see subsection 2.1.5) has already been established.

The following subsections describe different case designs (issues) and the corresponding results, followed by an analysis of both. These described issues have been executed one by one after each other. Therefore, the first issue has been executed first, the second issue has been executed second, and the third issue has been executed last. As the described issues will vary by multiple parameters, the analysis isolates the parameters and

its corresponding result as good as possible. Also, the changed policy has roughly the same amount of rules and impact to work behaviour to get a good comparable result.

All issues will follow almost the same security awareness cycle (see subsection 4.1.1) although there are a few differences, but will greatly differ in the *mindspace* parameters (see subsection 4.1.2). The differences in the security awareness cycle derive from an entanglement with the mindspace concept.

5.2.1 Target Audience

The target audience of this case study are all employees with an access to IT-devices of the company, respectively in need of IT to be able to accomplish their job. Therefore, all design elements, parameters, and media could be electronic. In fact, the issues always need an electronic medium to publish policies. The notification of policy changes often include electronic media. The survey of the case study, to gather data, is also done electronically and sent out electronically, as everyone included in the target audience has access to IT-devices and need to use them regularly to accomplish their jobs.

5.2.2 Security Awareness Cycle Parameters

The following paragraph explains the shared security awareness cycle:

- *Security Awareness Metrics* - The chosen metrics have already been described in section 4.3. They will be collected after each issue and evaluated afterwards.
- *Identify and Understand your Audience* - The audience(s) will be the same for each described issue. These groups are split into the already described standard users, power users, and administrators (see section 5.1).
- *Identify High-Risk and Desired Behaviour* - The high-risk behaviour and the desired ones are the sames, as the audience is identical, but differ per policy. The very same policy cannot be used twice on the same audience for exerimental results, as results will be disorted by the already established knowledge of the audience. In this issue study, a policy can therefore only be used once, as the audience stays the same. Therefore, these variances resulting from this difference are excluded in the analysis as good as possible.
- *Identify Solutions to Faciliate Behavioural Change* - The respective solutions depend on the respective policy. Therefore this variance is also excluded from the analysis.
- *Create Security Awareness Material* - The security awareness material is subject to the mindspace concept. The created material is assembled considering the various mindspace parameters. This step differs in the case study and is actively researched in the case study.
- *Deliver the Message* - The message, including the messenger, is part of the mindspace concept, so it differs and is researched in the case study.

5.2.3 Mindspace Parameters

The mindspace parameters allow a larger variation, than it it is possible to cover them all in a single case study. Some variations are explained in the organisations context in

the following list:

- *Messenger* - The messenger in delivering a new policy may be many people. There is the possiblility of the executive director, the information security manager, the manager of the respective department/division, a member of the information security team, or chosen ambassador of early adopters from the organisation. The executive director is the biggest display of authority. This may lead to a good result regarding autority-aware people, but may lead to a negative result regarding non-obedient people (libertines). Also, the executive director may not have the resources to present every relevant policy change. The information security manager may have such resources but lacks in authority compared to the executive director. The manager of the respective department may bring the message to its assigned employees. This manager should have resources to accomplish this. Also, this manager should be a trusted person, a "part of the crew", which also has some sort of authority. The member of the information security team may bring the most amount of knowledge to the message, but is probably not regarded as part of the employees team and also bears no authority. A team of ambassadors, which is trained by the information security team, may bring the message as a like-minded person, therefore in a friendly way, but has no authority.
- *Norms* - There are different norms in the organisation, which may seem quite common: e.g. eager to experience new things, don't change things that have "always" been that way. Both are present in the organisation. Also, the organisation is an Austrian organisation with a vast majority of Austrian employees, therefore, typical Austrian culture, a subset of European culture, is given.
- *Incentives* - They strongly relate to the individual person. Most of the policies created should be easily understandable and could be implemented in a private way as well. An incentive may be, that the policy guides you to a better and more secure private life and that the employees could use the same way at the workplace as well. There is no need to change behaviour when being on duty and in private life. Another incentive may be, to receive a clearly understandable policy, therefore, knowing exactly what is allowed to do. Another one is, that when complying to the policy, problems with any kind of authority is avoided. Furthermore, beeing needed to comply to something means, to be of value and importance to an organisation.
- *Defaults* - A policy may orchestrate work in a way that is absolutely exactly compliant to a regulation. Therefore, it wants to achieve a total compliance. Also, a policy may be adapted to the workflow. Therefore, it does not strives for total compliance but seeks to get people to adapt to the policy that does not completely changes their workflow. Also, it is different if the policy settings may be set to be the default setting in any technical settings, or if it is not. The location of publication of the policy may also differ to and focus on the people working on the policy or the people working according to the policy.
- *Salience* - To differ the salience paramenter, it is possible to notify all employees on a policy change, or only notify relevant stakeholders. Sending non-relevant messages to employees will result in a policy fatigue of these employees.
- *Priming* - There are different primings in the organisation. These are new and

already established employees; as well as power users and standard users (administrators may be power users as well as standard users, depending on their competence). New users do not have a priming at all while established ones do have a priming, power users do have a better understanding about an already existing policy than standard users.

- *Affect, Commitment, Ego* - These three parameters are regarded as a group. A competition, or a map exercise may push the ego of people, show deviations of the policy, create a challenge and commitment to solve this deviation and, therefore, gamify the process.

The case study was executed with a selection of one of the choices in these parameters.

Creating a new corresponding policy when merging two policies was a demand when doing the case study. This means the two or more corresponding policies are invalidated and a new unified policy is created including content of the invalidated ones and new content.

5.2.4 Description of Issue 1

The first issue is trying to change a policy in a majorly traditional way, which is constructed as followed. All new created policies are published via the already known procedures. That means, policies are published via the fileserver and the documentation system. Policies are always needed to be copied to both places. In this issue it means: create a policy in the *pdf* format and upload it to the documentation management system and export it to the file server. Merged policies will be deleted on both prior plattforms. When publishing, there is no exact documentation of change. There is only notice, that a change in the policy has happened, and there will be a very short, handwritten summary of the change. To carefully comply to a policy, it needs to be reread after every change by the relevant stakeholders. The notification of this change and its summary does not consider the competence nor the motivation of the audience. In fact, there will be no active notification at all.

The first issue has the following specific arrangement of mindspace parameters. An overview is described in Table 5.1.

As there is no active notification, there is also no dedicated messenger. T he messenger would be the creator of this policy, if someone asks specifically. There will be no drain of resources of higher level management and the messenger will deliver the message in a traditional way: “It has been decided by the management, so you have to apply to the new rules”. There are no specific measurements for an audience-aware language (cmp. section 4.2), when notifying and educating the employees, as there is no active notification and education about the change.

The norms taken in consideration are only the “traditional” Austrian culture of a little bit of complaining about everything, especially change [13]. There are no further differentiations made to other cultures and norms. Therefore, the policy change is executed by a “one norm fits all” approach.

The most incentives and also, the one that is communicated to the employees, to comply with the new policy is to not get into any trouble. “Comply with the policy, and you will have a happy working day.”

The defaults of work are not considered. The policy is written as if complied to it com-

pletely, theoretically there could be a total compliance to regulations itself. There are no considerations about working behaviour. The policy is published to the already known places, and splitted into sections compliant to the external standards and regulations; therefore, it is easy for the manager and the external auditor to explain and review the policy. Technical defaults are set to the policy, but this is done via best practice. There is no focus in supporting employees in complying with the policy technically, therefore, the technical IT team of the organisation has to read and understand the policy on their own and set defaults on their own.
All employees are notified on every policy change and have to decide on their own, if it is relevant to them. Their salience is not considered. The management decides, that all policies are relevant to everybody.
The policy changes are addressing already established employees. Their priming should be the already existing policy, which is changed at the moment. No further priming consideration about technical, legislative, or logical know-how are done.
The parameters affect, commitment, and ego are not considered much in this issue. The only affection of people is to not get into trouble (the incentive) and the anxiety to not comply to the policy (and getting caught). There is no public commitment, and there are no ego considerations.

Messenger	No dedicated messenger; creator is messenger when someone asks specific questions
Norms	Typical country norms
Incentives	Don't get into trouble
Defaults	Easy to read for InfoSec and auditor, no focus on workflow or technical defaults
Salience	Notify every change to everyone
Priming	Already established employees; they know about the existing policy, no further considerations
Affect	Get frightend when not complying
Commitment	None
Ego	None

Table 5.1: The mindspace parameters described for the first issue.

5.2.5 Description of Issue 2

The second issue is constructed as followed. All new created policies will only be published via the documentation management system. Merged policies will be deleted on both prior systems, which will eventually lead to the decommission of the fileserver/-folder. All stakeholders, respectively users that need to comply to the policy need to be aware of the new policy location. This documentation management system creates an

automatic versioning with a user-friendly diff (cmp. redline section 4.3). It is possible to create a watchlist per site/policy, which means everybody on that list gets notified per change with a diff provided. It is also possible for users to subscribe to that list themselves. A change notification is communicated to all people of the organisation reconcilement with the motivation and competence of the audience group.

The first issue will have the following specific arrangement of mindspace parameters. An overview is described in Table 5.2.
The messenger will be the information security manager. This messenger has a higher authority but no friendly relation to the respective departments. Also, the messenger needs to be aware of the different kinds of cognitive understanding and motivation of employees of a department to successfully deliver a message (see section 4.2). This may be a challenge to the single messenger, especially in larger organisations.
The norms taken in consideration are the country specific culture, as well as the "it has always been that way" culture and the "excited about new things" culture.
The incentive is to convince people, adapting to the wanted behaviour in private life helps them getting more secure themselves and they don't need to change behaviour if working and if not working. The incentives of this policy change may also get people to realise their value and importance to the organisation, which may boost their ego.
This issue strongly tries to adapt to the employees needs. Management and regulatories want the employees and the management to comply to regulations and policies, therefore, employees are a key part to achieve this. Employees need to be able to understand the policy and it needs to enable them their workflow. This approach does not seek for a total compliance of policies, but for a good comprehension of the critical parts of the policy and its total compliance of the critical parts. Therefore, the information security team educates the technical IT team about the policy and helps them in creating technical defaults compliant to the policy where possible. Also, the policy is created and maintained in a way, that an employee is able to quickly find the policy when needed. This means, that when in doubt, the policy is written for the employee, and the information security team including an external auditor need to search for information concerning any standard and external regulation. The work to search the correct terms is shifted to the creators and auditors.
This policy is drawn to everyones attention, as everybody gets notified. This leads to technical compliance (everyone was notified) but may result in some people tending to ignore this and further notifications.
As the messenger is only one person, the priming of other people is not considered differently. Therefore, the considered priming is in a low level prior understanding.
Affect is gained as well as the incentive. People realise their value to the organisation and may get a personal relationship to the organisation. This may also boost their commitment: Help the organisation to become resilient.
The commitment is created with a gamification of the policy change. Regularily, and after large changes, a map exercise is done in the organisation to experience the worth of the policy.
The ego is also pushed, when realising the worth of themselves in an organisation. Also, when participating in a map exercise, one could show its talents and prove its worth.

With this approach, the managers of the respective departments have a lot more to do than at the first issue. Although, this approach seems to cover more elements of the

Messenger	Information Security Manager
Norms	Typical country norms, “has always been that way”, and “ready to learn something new”
Incentives	apply same behaviour in private as in work; know your value in the organisation
Defaults	Easy to read for employees, focus on workflow and technical defaults, don’t focus on a total compliance but on critical components
Salience	Notify every change to everybody
Priming	Low level of prior understanding
Affect	know your value in the organisation
Commitment	regular map exercises
Ego	regular map exercises

Table 5.2: The mindspace parameters described for the second issue.

mindspace concept and also seems to still scale also with large organisations.

5.2.6 Description of Issue 3

The third issue has been similar to the second issue. It describes the notification of a policy made for a specific, larger audience group. In this audience group there are also different levels of characters, priming, social bonds, etc. Similar to the second issue, this policy also only gets published via the newly chosen platform, the documentation management system. All merged policy are deleted from their locations, leading to the decommission of the fileserver. Passive notifications are also done via the watchlist documentation (including the already described user-friendly diff), active notification is done via the messenger.

The messenger will be the manager of the respective department. Therefore, these managers will get notified and educated about the new policy by a member of the information security team. These managers then educate their departments about the new policies or policy changes. These managers as messengers take a key role in communicating the policy changes as many of the below parameters are transported by them.

The manager is the optimal person to address the employees of the department in the correct appropriate language (see section 4.2). The manager knows the people and their qualifications and therefore which language and motivation to use on which people. The typical country norms (“it has always been that way”) are considered and need to be overcome to successfully execute a change. It is necessary to endorse the minority norm (“try out something new”).
The incentive is to convince people, adapting to the wanted behaviour in private life helps them getting more secure themselves and they don’t need to change behaviour if

working and if not working. The incentives of this policy change may also get people to realise their value and importance to the organisation, which may boost their ego. Also, the incentive may be to try out something new, therefore, explore new ways.
The policy will be created to align to the already existing defaults. It is a permissive policy, that enables users to additionally do more things, than configured as the default. The default is also compliant to the policy.
To achieve the correct amount of salience, policy changes are only communicated to relevant people. This is achieved via the mentioned watchlist. Also, the automated diff helps in getting the relevant changes without the need to reread the whole policy.
Priming is also a parameter, which depends on the messenger. As there are different kinds of users (established employees, new employees, power user and standard users, the managers of the respective departments need to decide on their own how to deliver the messages. These primings may also be roughly divided into power users of policy A and standard users of policy B.
The affect is about the nature of this policy change. As it allows more possibilities to the employee, the employee might experiment with the new ways, but does not need to, as the default stays the same and is still allowed to do so. To summarise: Business as usual, unless you want to change it.
Commitment is especially created by employees that try out the new possibilities. As the old default is not changed, the other employees are not committed to the new policy, but probably won't jeopardise it either.
The ego may address people, that try out new ways and be able to present them to an audience of their choice. They might be seen as a pioneer.

Messenger	Managers of the respective department
Norms	Typical country norms, "has always been that way", and "ready to learn something new"
Incentives	apply same behaviour in private as in work; know your value in the organisation; explore new ways
Defaults	Align policy to default. Expand permissions to users beyond the default.
Salience	Notify every change to relevant people and interested parties only
Priming	Already established employees and new employees, power users and standard users
Affect	Be able to experiment, but not necessary to do so
Commitment	Commit to the new possibilities if you use them, don't jeopardise if you do not use them
Ego	Try out new things, be a pioneer

Table 5.3: The mindspace parameters described for the third issue.

5.2.7 Used Metrics and Measurements

This case study focuses on the communication and education of policy changes to employees. It also tries to simplify policies to a better readability and comprehension to employees. The main focus is to measure and analyse the different communication parameters to notify and educate employees about an information security policy change. The varying parameters are derived from the framework mindspace, while the metrics, that are used to measure the varying output of the mindspace parameters, are created within this thesis. The required and used metrics in this case study are derived by the metrics mentioned in section 4.3:

- *Policy Redundancy* is a metric which is useful to measure the entire set. As the case study only regards a subset (two policies), the metric is not appropriated and will not be used.
- *Comprehensability* can be measured during the observation period. The comprehensability is a powerful metric but needs to be measured in combination with implementability and applicability, low questions may also indicate that less people read the current policy. Comprehensability is measured in the number of people who rate a policy as easy to read and/or understand.
- *Implementation and Applicability* is a metric that counts all policy violations that have been observed and/or reported. There is no need that these violations already have created an incident. This metric may be abbreviated to *Implementability* or *Implementation* in the following paragraphs.
- *Incidents* are also counted. An incident may arise from a policy violation, but may also start from an event, that is not covered by the policy at all. This will lead to maintainability.
- *Maintainability* is measured by the amount of time (in hours) that is needed to maintain and adapt the policy due to questions (*comprehensability*), policy violations (*implementation and applicability*), and notable security events (*incidents*).
- *Recommendation* is a semi quantitative metric as it only allows two results (yes/no) and, therefore, it is a boolean metric. It measures the quality and effectiveness of the chosen issue and is measured by the author.
- *Improvement* is also a qualitative metric. It does not count the number of improvements, this is indirectly measured in the maintainability metric. It is a list of possible, feasible improvements that may be done in a further attempt.
- *Understanding* is also a qualitative metric, but not evaluated by the author, but by the employees. They rate the policy on its applicability in their workflow.

Additionally, another metric *Awareness* has been questioned. This metrics measures, if people know, that a policy exists. Table 5.4 summarises these metrics.

These metrics are used to measure the communication of changes of the information security politics to employees, as these are the people relevant to implement a regulation-compliant workflow.

Used Metric	Time of Measurement	Type	Description
Policy Redundancy	not measured	quantitative	Which policies are redundant? Not appropriate/used in case study.
Comprehensability	during case study	quantitative	Is the policy easy to read/understand?
Implementation	during case study	quantitative	How many policy violations have been noticed? (Full name of metric is Implementation and Applicability)
Incidents	during case study	quantitative	How many incidents have been recorded?
Maintainability	after analysis	quantitative	How much time is needed to maintain the policy?
Recommendation	after analysis	semi quantitative	Is the approach recommended?
Improvement	after analysis	qualitative	What could be improved?
Understanding	during case study	qualitative	Applicability on workflow
Awareness	during case study	quantitative	Do people know that the policy exist?

Table 5.4: This table summarises the used metrics, their type and their time of measurement.

5.3 Data collection

This section describes the measured metrics and results of the case study issues described in section 5.2. The metrics *Comprehensability* and *Understanding* have been collected via a survey distributed to the relevant people in the organisation via an electronic

medium. This survey questioned the people if a policy is

1. known
2. easy to understand
3. subject to questions

These questions had predefined answers to allow a quantitative research. The survey was answered by 48 people (cmp. section 5.2: 200 employee total, 50 employees working with IT-assets) within a week and was unsupervised.

The metrics *Recommendation*, *Maintainability* and *Improvement* will be measured after the analysis of the case study issues (see Table 5.4).

All other metrics have been collected via review of the event documentation system of the organisation and interviewing the relevant personnel. These experts have been chosen based on their knowledge of information security in general, knowledge of information security processes, guidelines and policies in the organisation, and knowledge of workflows and incidents in the organisation. There have been two interviews with one interview partner each. Both were asked the same questions to get a list of relevant policy violations regarding the specific policies in the specific timeframe. The gathered lists have been deduplicated, cleaned, and enriched with documented policy violations from the documentation system. The resulting amount represents the metric *Implementation and Applicability*.

5.3.1 Issue 1

The first issue was executed as described in subsection 5.2.4. The following metrics have been measured:

Awareness	37
Comprehensability	28
Implementation and Applicability	31
Incidents	5
Understanding	hard to find changes, read but not implemented

Table 5.5: The measured metrics of the first issue

5.3.2 Issue 2

The second issue was executed as described in subsection 5.2.5. The following metrics have been measured:

Awareness	22
Comprehensability	11
Implementation and Applicability	3
Incidents	0
Understanding	complex, accessable

Table 5.6: The measured metrics of the second issue

5.3.3 Issue 3

The third issue was executed as described in subsection 5.2.6. This policy only addresses and applies to 27 employees (all with IT-assets) in the organisation. 15 people conducted in the survey. The following metrics have been measured:

Awareness	9
Comprehensability	6
Implementation and Applicability	2
Incidents	0
Understanding	applicable, enabling, easy to understand

Table 5.7: The measured metrics of the third issue

5.4 Analysis

The different parameter sets of the test issues resulted in different outcome during the case study (see section 5.3). The following subsections discuss the outcomes, their possible causes, and answer the last metrics *Improvement* and *Recommendation*. The survey was conducted with 24% of the total of the employees which is a quite big sample. 31.25% people of the target audience are part of the sample. The sample group is regarded as representative to the organisation and its target audience of the policies.

5.4.1 Issue 1

Issue 1 described a change of a fundamental of the information security framework. 77.08% (37 people) of the surveyed people answered to have knowledge about this new policy, whereas 56.25% (27 people) answered that they only noticed the new policy via the documentation mangement system, 6.25% (3 people) answered they only noticed the new policy via the fileserver and 14.58% (7 people) answered that they know the new policy from both locations. Interestingly, the vast majority of people noticed the policy via the new location (documentation management system), while a small amount noticed them via both location and only a small minority still found the policy only via the old location (fileserver). This may indicate, that people are either already trained to

look into the documentation management system, or they simply prefer the advantages of the system or both. The fileserver itself is only used very little.

75.67% (28 people) of the people who noticed the policy answered that the policy is easy to understand. This is remarkable, as there were 31 reported or noticed policy violations and 5 reported incidents in the surveyed time frame. The high number of people who answered to understand the policy and also the high number of violations and incidents may either indicate a misunderstanding of the policy (*comprehensability*), people simply ignoring it (*applicability*), people not being aware of the policy while working, or a combination of both. The qualitative feedback, that was given, was that it was hard to find changes, and most people only read the policy but did not actively comply to it. This also indicates, that the policy is not very applicable and may be a reason that explains the high number of policy violations and incidents. This might origin in the short, handwritten changelogs and the inability of the documentation management system of creating detailed changelogs of a *pdf* format: ergo there was no comprehensive changelog.

Analysis of Audience-Aware Language

In this issue did not focus at all onto the correct audience-aware language. Some people may have understood the message by addressing them correctly by coincidence, but most people probably have not had understood the message correctly. This may be indicated by the high amount of people, that answered that they knew about the policy and they understood it, but still a lot of policy violations and incidents happened.

Analysis of Mindspace Parameters

There has not been a real messenger, in fact the policy was simply changed without adequately notifying employees. This may indicate that employees did not notice the change at all. Long term employees still applied an old version of the policy while new employees might have applied to a newer version. This varies based on the manager of the employee and the motivation of the employee. If the manager did not notice the change, the new employee was taught an old version of the policy. A motivated employee might have implemented a new version because of a first lecture of the current version at the time of employment. The lack of notification of change also shows another problem: All employees knew the policy in a different version based on their education and/or employment. Since there was no notification, employees did not update their knowledge of the policy. This may explain the high awareness and comprehension rate, but nevertheless also the high policy violations and incidents rate (see Figure 5.1 and Figure 5.2). People knew the policy and understood it, but were not aware of an update and therefore new rules to obey.

No specific norms, except for general country norms, have been taken into consideration. There has not been a differentiation of white collar and blue collar people, or any differentiation in any department concerning communication and language used. As there also hasn't been a messenger, the changes have not reached the employees and were therefore not implemented.

The only incentive used, was that employees will get into trouble if they won't implement the policy. This negative, non-enabling, non-embracing incentive may be

seen as an analogy to law enforcement. Punishments work preventive up to a specific level, but do not guarantee a full compliance to rules [2]. This may be seen in this issue as well. A positive, embracing incentive, something that has a positive effect on the actor may improve compliance.

This policy was written primarily for the auditor and the information security management team, but not for the employees in need of implementing them. There are no references to workflows, no guidelines or examples provided. There is no technical default provided to comply to this policy. The employees implementing the policy do not get any help in form of defaults. They often also do not know where to look for a rule as the policy does not have any references to the workflow or produced products.

Also, as a controversy to the messenger parameter, every change is communicated to the addressed receipients. Therefore, receipients that did get notified, got all changes to every details, including non-content changes (e.g. formatting issues). This may contribute to a readers fatigue, that readers miss relevant changes. This behaviour is also known as operators fatigue in operational information security. An attacker permanently issues a specific false positive to fatigue the operator and launches an attack over this exact vector after some time passed [59]. Reducing notifications to a minimum, summarising the change and only notify when relevant changes have been done, helps in reducing the fatigue.

The priming of the policy changes are based of the knowledge of the long term employees. They already knew about the policy framework, knew the policies and needed to adapt them after a change. New employees were not adressed at the change, as they are supposed to learn the new policy as part of their employment anyway. This may be a reasonable consideration, but since the changes were not communicated to the receipients properly (missing messenger), this cannot be validated.

The only emotion bound to this policy and its change was the fear of non-compliance. Similar to the incentive parameter, there was only a negative binding and no positive one. The same analogy to law enforcement could be found for this parameter. A positive emotion may increase policy compliance and therefore lower the policy violation and incident rate.

No commitments have been created, as well as no ego has been adressed. Employees did not feel associated with neither the policy nor the change. This is also a parameter that explains the high rate of policy violations and incidents. A public commitment and ego boosting actions may have lowered this rate effectively.

It is assumed, that since the employees already knew a version of the policy and did not get a comprehensive changelog, they simply applied to the old version of the policy. This resulted in the high number of policy violations and incidents.

The missing messenger is a critical part of the change. Without a messenger, the message about the change cannot be delivered to the respective employees and, therefore, the change cannot be implemented. This leaded to a highly diverse understanding of the policy and a high number of policy violations and incidents. The missing positive emotions, the non-association of the employees to the policy, the missing defaults, and the operators fatigue due to notifications about every detail also played a part in the low performance of issue 1.

Collection of Metrics

As mentioned in subsection 5.2.7 metrics have been collected after the analysis of the issue. This is done in the following paragraphs regarding issue 1 and summarised in Table 5.8.

The improvements based on the analysis above are to assign a messenger to a policy change and let the messenger deliver relevant changes to the correct relevant stakeholders in their language. Also, enrich the message with positive emotions.

The recommendation, based on the analysis above, is *no*. Not having a messenger and, therefore, no message is a critical failure of this issue. The result of employees not knowing the version of a policy is in effect and, therefore, a resulting non-compliance is the contrary of the goal "a successful merger".

Improvement	Assign a messenger, attach positive emotions to the message
Recommendation	no

Table 5.8: The measured metrics of the first issue after analysing it.

5.4.2 Issue 2

Issue 2 described a change in another fundamental policy of the information security framework. The answers were quite different, than the ones given to issue 1. Only 45.83% (22 people) answered that they knew that the new policy exists. This policy was only available via the documentation management system, there was no publication on the fileserver. Interestingly, many people of the audience were aware of the policy of issue 1 because of the documentation management system, while not so many were aware of the policy of issue 2. It is assumed, that the awareness of a policy does not fully correlate to the location but more to the notification of a change. Nevertheless, the location is relevant in placing and publishing a policy, as it is important to use a system which is used by employees regularily.

Also, only 50% (11 people) of the people who noticed the policy answered that it is easy to understand (*comprehensability*). 3 policy violations (*applicability*) have been recorded and/or noticed and 0 incidents happened. Despite the low awareness and understandable rate, compared to issue 1, there are very few violations and no incidents, therefore it seams, that the policy is written in a default way. The qualitative feedback, that was given, was that it is a complex policy, but ready by default (therefore there is "nothing to do" when doing standard tasks, and it is easy to access it. Enabling a policy ready by default is convenient in the daily work, but bears the risk, that one simple forgets about the relevant policy, if it is not a default task and therefore a non default action needs to be taken.

Analysis of Audience-Aware Language

This issue already tried to take the audience-aware language in account. The manager of the information security department tried to address everyone on their level and motivation. This seems to work as the policy violations and incidents were significantly lower

than at issue 1 (see Figure 5.2), but may still be improved. The manager of the infosec department does not seem to be the best messenger for the whole organisation. The very low awareness and understanding rates seem to be rooting from another problem.

Analysis of Mindspace Parameters

This issue had a dedicated messenger, the information security manager of the organisation. The information security manager also did deliver the message to the employees, therefore, people had a chance to notice a policy change and could notice their need to reread the relevant parts of the policy. Nevertheless, the awareness rate is rather low and so is the comprehensability rate (see Figure 5.1). This is impressive, because although people answered that they do not know about the policy - and those who do, do not understand it - people still correctly implemented the policy, as there is a rather low policy violation and incident rate. There are two explanations for this phenomen:

1. The policy is written in a very default way.
2. People do know the principles, but do not know it as this policy.

Therefore, people do not need to know about the policy and its content, as they apply it as part of their common sense and part of the companies common sense.

The used norms only differ a little bit to issue 1. There are also the typical country norms that are adressed, as well as an “it has always been that way, therefore we do not change it”, and a “ready to learn something new” culture. There were no considerations on white and blue collar workers. The only real difference was, that motivated workers were also considered in the message.

The incentive used enables employees to use the exact same behaviour also at home and in private in general. The policy was written to enable the employee to effectively improve security of the workplace as well as their private live. The low policy violation rate and incident rate may validate this statement.

This policy and the message of the change did focus on creating and maintaining a useful default. The default lets employees focus on the non-changed workflow and on critical components. This also lead to a compliant workflow as pictured in Figure 5.2. People complied to the policy, especially at the critical parts, as it is in a default way, and people did not think about the policy much. This behaviour might lead to problems, when a non-standard workflow is required.

Equally to issue 1, every change had been communicated to the addressed receipients. This included every change at every detail level, including non-content changes (e.g. formatting issues). Like at issue 1, these notifications may contribute to a readers fatigue, that readers miss relevant changes. This behaviour is also known as operators fatigue in operational information security. An attacker permanently issues a specific false positive to fatigue the operator and launches an attack over this exact vector after some time passed [59]. Reducing notifications to a minimum, summarising the change and only notify when relevant changes have been done, helps in reducing the fatigue.

The priming of the change of this issue focused on a low level of prior understanding. This addressed newly recruited people, as well as security-unaware people, but will probably bore already established employees, as they know the topic. Bored employees are less likely to notice or remember relevant changes of a policy.

The affect used is quite positive. The message focused on creating a binding to the

organisation due to increasing the knowledge and awareness of the employees of their value to the organisation. People see, that they play a critical part inside the organisation and that the organisation needs the employees in their positions to function correctly. These positive emotions increase the learning effect and the willingness to learn and comply to new policies and guidelines.

The commitment to this change is rather low. There has been a map exercise, to gamify the policy and to show its usefullness to the players. Also, the players learned how to implement and comply to the new policy. This map exercise did only create a weak public commitment, however. Although, the boost on the ego may increase significantly, if employees could demonstrate their knowledge and skills during these map exercises publicly.

This issue has the vast advantage of having a technical and organisatorical default, which leads to a lower policy violation and incident rate as people comply to it by default. There are two disadvantages of this approach:

- Knowledge about the policy may get lost, as it is not used consciously.
- Policy violations may happen unnoticed, when a non-default event is handled in a default way.

Also, the message had a messenger. These parameters are a key in the overall good performance of issue 2 (see Figure 5.1 and Figure 5.2).

Collection of Metrics

As mentioned in subsection 5.2.7 some metrics have been collected after the analysis of the issue. Again, this is done in the following paragraphs regarding issue 2 and summarised in Table 5.9.

There are two improvements based on the analysis above:

- to assign a messenger that has a better connection to the respective departments. Also, this scales better in terms of time resources.
- to notify relevant receipient based on their notification preferences, on default only notify relevant changes.

The recommendation based on the analysis above results is a *yes*. This approach proved to be working and effective, although there is still a lot of potential to improvements.

Improvement	Assign a messenger from the respective departments, reduce notifications to a relevant minimum
Recommendation	yes

Table 5.9: The measured metrics of the second issue after analysing it.

5.4.3 Issue 3

Issue 3 described a change in an optional, enabling policy only addressing a subset of the employees (27 of 200 people) of the organisation. This circumstance has been

addressed in the survey of the employees. 15 people (31.25%) of the participating 48 people were in that group. The target audience was IT-aware and worked a lot with the documentation management system. 60% (9 people) answered that they know that the policy exists. This policy was also only available via the document management system, which was the primary documentation system for the target audience. Also, the people of this audience never accessed policies via the fileserver.

66.7% (6 people) of the aware people answered that the policy is easy to read and understandable (*comprehensability*). 2 policy violations (*applicability*) have been recorded and no incidents happened. The qualitative feedback, that was given, was that it is an applicable, enabling, and easy to understand policy. The low comprehensability rate contradicts the measurement "easy to understand", but it needs also to be beared in mind that the quantity of the feedback (9 people were aware of the policy) is rather low. This policy was an enabling one, therefore, it allowed another defined workflow besides the default one. Therefore, it only applied to people wanting to work aside the default workflow.

Analysis of Audience-Aware Language

This issue addressed the audience-aware language seriously. The respective managers of the departments delivered the message in their language and tried to translate it to the languages and motivations of their employees. This resulted in the best policy violation and incident metrics. The metrics are quite similar to issue 2, as they are both on a very low level. Therefore, this may be a measurement inaccuracy. Also, the low awareness and understanding rates seem to have a different origin.

Analysis of Mindspace Parameters

This approach made use of multiple messengers, the manager of the respective departments. This allowed two things:

- scaling time resources based on the organisation needs
- approaching the message to the employees in their known way and in their appropriate language

The time needed to address all employees is scaled out to their respective managers. There was no single person, that was responsible to deliver the message to all employees. Also, the respective manager was able to deliver the message in the way and language that was needed in the department. The manager knowed the employees and knowed in which way a message is delivered best.

The norms used are identically to issue 2. There were the typical country norms, as well as the "it has always been that way, no need to change it", and the "ready to learn something new" culture that had been addressed. Similar to issue 1 and 2, there were no considerations made about blue and white collar workers. As this policy only addressed white collar workers, there is no need to do so.

This message had multiple incentives for the employees. The first incentive was to be able to use the same behaviour in private life as well as in busines context. Therefore, there was no need to switch behaviour in the different kinds of context. Using this behaviour in private life may improve private security as well as the organisation. The

second incentive was, similar to issue 2, that employees learned about their value to the company that they provide. The third incentive was, that the employees were able to explore new ways of working. This incentive works best with people which are related to the "ready to learn something new" culture.

This policy change expanded the default. Therefore, there was a technical and organisatorical default which was compliant to a policy, but this policy change covered non-default workflows. In combination with the publishing of the policy change, there had been a publishing of a non-default workflow compliant to this change. Therefore, there was a live example on how to implement this policy change which may be viewed as default.

This policy change was notified to relevant people only. Therefore, there was an addressed audience, and only that audience got notifications about the relevant change (27 people out of 200; see section 5.3). This reduced policy fatiguees, as people did not get notified about changes of non-relevant policies.

The priming of this policy change focused on already established employees, but also addressed new employees. The focus on the already established employees was merely because new employees needed to learn the new policy framework during employment. They needed to change their workflow fundamentally in order to work for the new organisation. Already established employees needed to know the exact changes, as they already knew the previous policy. There was also a differenciation between power user and standard user (cmp. subsection 5.1.1), therefore, the policy language and language of the change message tried to address both. Both user groups were represented in the audience group, therefore both needed to be addressed.

The affection of employees to this policy change was very positive as it enabled them to choose between workflows. They were enabled to experiment, but they did not need to. This circumstance should have been communicated as it pleased people sticking with the default and people that did not want to stick to the default but to experiment with new things.

The commitment was also quite clear. The public commitment was to comply to the new policy change if it was used, but also to not jeopardise them if it was not used.

This issue addressed the ego quite positive, as it enabled people to be a pioneer and to experiment, explore with workflows. Successful experimentations could have been made public and referenced to the employees that were responsible to discover them.

This policy change was very successful as it had an overall acceptable awareness and comprehensability rate, but a very low policy violations and incident rate (see Figure 5.1 and Figure 5.2). This may be a part of the scaled messenger concept, as well as the positive incentives, predefined defaults and positive personal effects. Although the good performance of this approach, it consumed the most initial time resources when preparing the policy change and message.

Collection of Metrics

As mentioned in subsection 5.2.7 some metrics have been collected after the analysis of the issue. Also, for issue 3, this is done in the following paragraphs and summarised in Table 5.10.

As the awareness and comprehensability rate of this issue is not as high as expected,

there are two improvements based on the analysis above:

- to improve the salience parameter. People need to be aware of the policy change. Therefore, adjustments need to be done on the salience parameter.
- to improve the priming parameter. The message needs to be better prepared to be readable and understandable by the various user groups.

The recommendation based on the analysis above results is a definitive *yes*. This approach proved to be working and effective, although it is time consuming in the beginning. There is no research being done about time resource consumption of the maintainance in this case study.

Improvement	improve salience and improve priming
Recommendation	yes

Table 5.10: The measured metrics of the third issue after analysing it.

5.4.4 Comparision of the issues

All three issues have been done within a timeframe of 1 year whereas the respective starts have been diversived per issue. Each issue has been measured during the first six months after the change of the respective policy. The measures and analysis of each issue has been done in the paragraphs above. Next, a comparision of these issues follows.

All issues have a distinctive set of mindspace parameters, place of publication, method of notification, and used language. These differences have created different results which are shown in Figure 5.1 and Figure 5.2.

After the analysis of the issues, some more metrics have been gathered which are summarised in Table 5.11.

Awareness

Issue 1 has the best awareness score, followed by issue 3 and issue 2. The awareness is measuring if people know the policy and the change. This high score at issue 1 needs to be qualified as the policy of issue 1 is the oldest policy iteration. As the policy change in issue 1 was not anounced and most people did not get notified, it is assumed that most people did not notice that change. Therefore, it is assumed that people answered that they know the policy, not the change. It is also supposed, that, through this guessed behaviour, the awareness measurements of issue 1 were unintendedly forged to result in a better score.

The low rate of issue 2 may be explained, that people did not know that the policy exists as it may seem to be common sense, and it is the default workflow. Therefore, people applied to the policy but are not aware, that there is a policy about it, although there were specific notifications about the policy change. It is assumed, that people tend to forget common sense policies, as they comply to them either way as part of the default workflow. This behaviour needs to be evaluated, as it may be crucial knowledge when changing the policy to a non-default, non-common-sense policy.

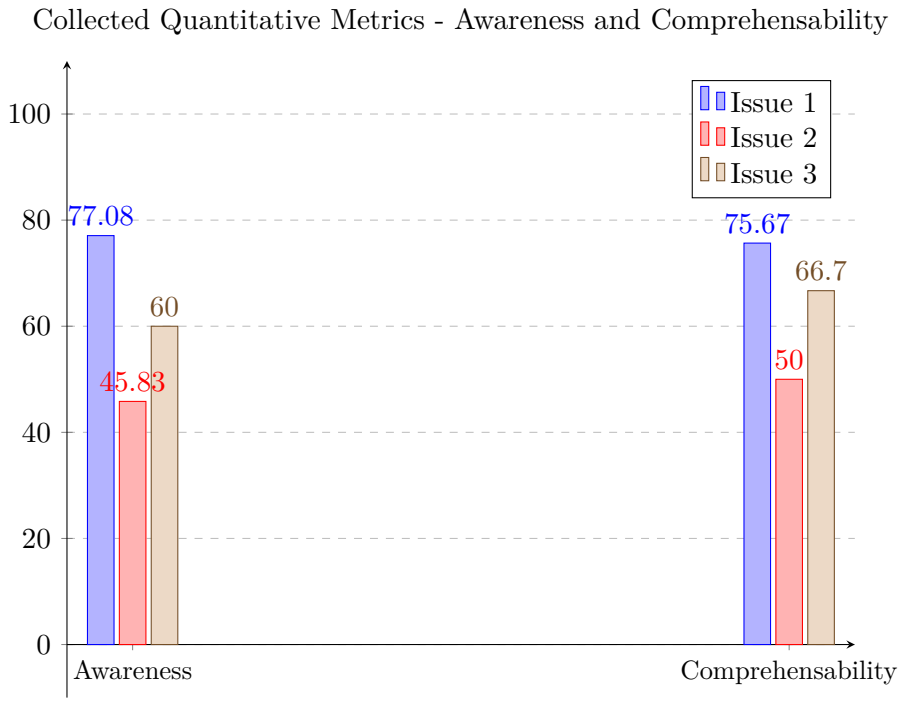

Figure 5.1: The figure displays the collected metrics *Awareness* and *Comprehensability* of the case study. The data of the metrics has been normalised between the different issues and is displayed in percentage (see subsection 5.4.1, subsection 5.4.2, and subsection 5.4.3). The first bar at every parameter represents issue 1, the second bar represents issue 2, and the third bar represents issue 3. These metrics aim for a 100%. Also, the metrics *Awareness* and *Comprehensability* are results of a self assessment of the employees.

Issue 3 had been a new policy, therefore the change in the policy framework was the creation of this policy. There are no misunderstandings of old and new policy versions, therefore, this rate is also solid.

Comprehensability

Issue 1 has the best comprehensability score, followed again by issue 3 and issue 2, but with the same problem as with the awareness score. People did not notice the change and still think of the comprehensability of the old version of the policy. Therefore, the score may give a rough feeling of the actual situation but it is not accurate. Nevertheless, the score of this issue has the potential to be improved.

Issue 2 has the lowest score. People, that were aware of the policy change did rate this policy as hard to read and understand. People also noted, that this change and policy is quite complex (metric *understanding*). The messenger may not have found the correct audience-aware language. Also, this score is quite low, as the change of this issue needs to be improved significantly in this metric.

Issue 3 has a score right in between issue 1 and issue 2. It is hard to analyse that low score, as people answered, that this change and policy is “easy to understand” (metric *understanding*). Also, the messenger of the change was the respective manager of the

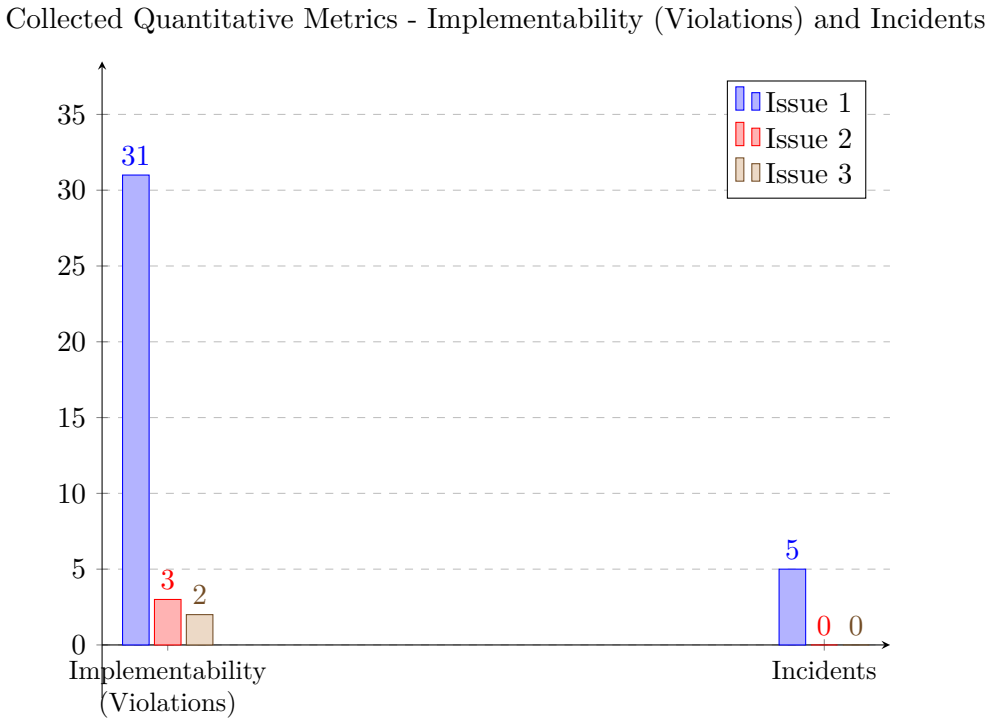

Figure 5.2: The figure displays the collected metrics *Implementability* and *Incidents*. The displayed numbers are absolute numbers (see subsection 5.4.1, subsection 5.4.2, and subsection 5.4.3). The first bar at every parameter represents issue 1, the second bar represents issue 2, and the third bar represents issue 3. These metrics aim for zero occurences. Also, the metrics *Implementability* and *Incidents* are an observation of the organisation.

departments, which should be able to use the appropriate language per audience. It is possible, that the messenger may not have understood the policy change correctly.

Implementability

Issue 1 has the most noted policy violations and, therefore, the worst implementability score. As people did not notice the change, they still apply to the old policy version which leads to a lot of policy violations.

Issue 2 and 3 have a quite similar score which is very low. These policy violations could be negligible as there are so few. There will always be policy violations in some kind, but the number of them should stay low. The low number could be explained by the fact, that the policy is either in a very default way, or an optional, enabling policy with a lower number of users.

Incidents

Issue 1 has the most incidents, therefore events that happened because of a policy violation that had an impact on the information security of the organisation. The incident rate is the worst compared to the other issues. This could be explained by the high

number of policy violations and the fact, that people did not know that there was a change.

Issue 2 and 3 do not have any incidents related to them. This is the optimal score. Similar to issue 1, the low rate of incidents are explained by the low number of policy violations.

Issues	Recommendation	Improvement
Issue 1	no	Assign a messenger, attach positive emotions to the message
Issue 2	yes	Assign a messenger from the respective departments, reduce notifications to a relevant minimum
Issue 3	yes	improve salience and improve priming

Table 5.11: The collected metrics after the analysation of the various issues. The metric *Recommendation* is a semi quantitative metric, telling if the author of the thesis recommends to implement a change according to the parameters of this issue. *Improvement* are recommendations to what could be improved when redoing these issues.

Improvement

Issue 1 needs to be improved by assigning a messenger to the change. This messenger needs to notify the respective people about the change. Without a messenger, people do not notice the change and, therefore, cannot apply to it. The vast majority of negative measurements of issue 1 are related to the missing messenger. Also, positive emotions attached to the message may improve its effects.

Issue 2 had a messenger, but it was a single person. The notification of change should be delivered by multiple messengers from the respective departments to apply the appropriate audience-aware language to the message. Also, employees feel more connected to the messenger of their own department as to other people. Another improvement is to reduce notifications of changes to a minimum, that only relevant changes are announced.

Issue 3 has a low salience performance which means that there should be more notifications. Some people did not notice the policy change. Also, the priming of the audience needs to be more in focus when creating the message. People did not understand the message based on their prior knowledge of the topic.

Recommendation

Issue 1 is not recommended to be applied in organisations. The results of the case study are quite low. The major flaw of this issue is that people did not notice the change of the policy and, therefore, still work with the old policy version in mind. This behaviour makes all further changes obsolete, as they are not implemented into the workflow and only exists on paper.

Issue 2 is recommended to do so. Issue 2 has good scores at the different metrics, although there are possible improvements at the notification level. As issue 2 works

on a good default, people instinctively do the right thing. Although, the policy change itself, the communication part, was not that successfully as seen at the awareness and comprehensability score.

Issue 3 is also recommended to be applied in organisations. The effectiveness of the change is as good as at issue 2, but it did the communication part significantly better. Although there still exists some improvements, issue 3 has the best score overall.

5.5 Comparison with the hypothesis

The hypothesis as mentioned in section 4.4 is quite similar to issue 3. The following list compares the hypothesis to issue 3 and analyses it. The list items are aligned to the list of section 4.4.

1. Issue 3 published the policies via a documentation management system which supports automatic versioning. This versioning is quite easy to use, although it is unknown if users know about this feature.
2. The used documentation management system offers automatic notifications via email. As email is the most important messaging tool in the organisation at the moment, this is a good approach to send notifications. To receive notification, users need to subscribe to the groups of documents or the documents itself. Also, this is very easy to use, although it is unknown if users know about this feature.
3. The messenger of issue 3 was the manager of the respective department.
4. Issue 3 addressed both norms, but encouraged the “try out new things” norm.
5. This issue also offered a positive incentive: to actively improve the security of the company and of private life.
6. The policy was offering another workflow, different from the default. Defaults for the alternate way needed to be developped by the users. A very default aware policy change was done in issue 2.
7. Subscribed users did get notified about every single change. Relevant changes were communicated to relevant stakeholders via a messenger (the managers of the respective departments).
8. This issue focused on already established employees, but also addressed new employees. It also addresses the different user groups (see subsection 5.1.1).
9. Happy emotions were created via enabling users to experiment if they want to.
10. The commitments were not public. Also, the commitment is more about not to jeopardise employees if they want to use policy features.
11. The ego is boosted via enabling employees to be a pioneer and explore, experiment, and establish new workflows.

As issue 3 has the best performance score overall, and aligns best with the hypothesis, it is assumed that the hypothesis is quite accurate. As issue 3 still has potential to improve, this is explained that issue 3 did not align to the hypothesis 100 percent.

Chapter 6

Closing Remarks

This thesis studies the merging if information security policy frameworks and effectively communicating the change to relevant stakeholders.

6.1 Research Questions

The thesis has one main and an intermediate research question (cmp. section 1.5). The intermediate research question about the measurements has been answered in subsection 5.2.7, although the metric *maintainability* has not been analysed. The gathered data for this metric was qualitatively low and could not be analysed and compared. The answer to the main research question was created in section 4.4 and validated in section 5.5. The key points of the research are summarised in the following list.

1. Assign a messenger to all relevant changes. Without a messenger there is no message, and therefore no notification of a change. The research in this work has shown that a non-notified change was typically not implemented into the workflow and was therefore worthless for the organisation.
2. Use audience aware language. The audience needs to understand the message, that the messenger is trying to announce. Each audience had its own specialisation and its own language. The message needed to be delivered in the language used by the audience to them to understand it correctly.
3. The messenger needs to understand the message. Correctly delivered messages and correctly translated messages needed to be understood by the messenger.
4. Publish documents that support automatic versioning. This helps people to focus on the change of a policy and, therefore, notice relevant novelties. Automatic notifications supported people to keep the pace of policy changes. Relevant changes needed to be announced via a messenger.

Three issues have been examined, where issue 3 fulfilled the previous described key points of the thesis the most. The very good performance of issue 3 and the high alignment of the parameters of issue 3 with the hypothesis support the validity of the hypothesis.

6.2 Metrics

The awareness metric has been shown to be a powerful metric to collect if people even noticed a policy change. If people did not notice change, all other metrics are not relevant, as they require people to know that change happened. When collecting this metric via a survey, it is important to point out to the audience, that only the change itself is relevant for the survey, not the policy itself. This was opaque at issue 1.

The comprehensability metric is a metric that may indicate the understanding of the policy. It is similar to the understanding metric. Both metrics contradicted each other in the case study, as people answered contradicting on the questionaire. As a quantitative metric, the comprehensability metric has enabled a better comparability to the other issues as the understanding metric, but the understanding metric may provide better answers to the research question.

The implementation and incident metric were powerful metrics to measure the results of a change, as they do not ask people about their evaluation, but they count actual events. They also differ if an event is only a violation, or if the event damaged to the organisation.

The metrics improvement and recommendation are metrics that were collected after the analysis of the issues and describe possible improvements of the issues and if the issue is recommended to be implemented in an organisation.

The metrics policy redundancy and maintainability have not been gathered respectively analysed. The policy redundancy has not been suitable to this thesis, as the thesis only compared distinctive policies but the metric would compare the policy frameworks. If comparing the policy framework, this metric could be powerful to measure the effectiveness of the structure to create and maintain the framework. The metric maintainability was meant to measure the sustainability of the policy, but could not be evaluated due to opaque answers. This metric needs a revision.

6.3 General Observations

The case study showed the effectiveness of the various parameters of the mindspace framework, in combination with audience-aware language and searchable, versioned documents. Mindspace is a powerful tool to adjust communication, while audience-aware language helps delivering the correct message. The searchable, versioned documents support the employees to notice relevant changes. The ideal change should be accompagned by a versioned document, and a message that is understood by the audience that is transported via a known, friendly messenger, attributed with personal incentives and positive emotions. Mindspace is a promising framework to create effective communication about information security policy changes.

Tuning the salience parameter (cmp. subsection 4.1.2) was quite difficult. Creating to many notifications had a similar negative impact on the performance of the change of a policy as creating to few notifications (see subsection 5.4.4).

Using nudging is an ethically discussed topic. Adapting policies, tools, and options to the cognitive skills of employees is a requirement. Nudging should only get used in ethically non-ambiguous situations, like improving security of an organisation via policies.

6.4 Future Work

Another experiment or case study needs to be done in another organisation to get comparable results. Also, there should be an experiment, that totally aligns to the hypothesis. This could either validate the hypothesis completely or show errornous assumptions. The hypothesis will probably support further mergers in a positive way, but more research needs to be done to validate this statement. The gathered results of awareness and comprehensability (see Figure 5.1) should be subject to improvement.

References

Literature

[1] Sherly Abraham. "Information Security Behavior: Factors and Research Directions". In: *A Renaissance of Information Technology for Sustainability and Global Competitiveness. 17th Americas Conference on Information Systems, AMCIS 2011, Detroit, Michigan, USA, August 4-8 2011*. Ed. by Vallabh Sambamurthy and Mohan Tanniru. Detroit: Association for Information Systems, 2011. URL: http://aisel.aisnet.org/amcis2011%5C_submissions/462 (cit. on p. 5).

[2] Johannes Andenaes. "General preventive effects of punishment". *U. Pa. L. Rev.* 114 (1965), p. 949. DOI: https://doi.org/10.2307/3310845 (cit. on p. 39).

[3] Isaac Asimov. *Runaround*. Street & Smith, Mar. 1942 (cit. on p. 4).

[4] R.E. Baida. "Merging Prioritized Security Policies". In: *International Conference on Digital Telecommunications (ICDT'06)*. 2006, pp. 50–50. DOI: 10.1109/ICDT.2006.48 (cit. on pp. 2, 15).

[5] Béatrix Barafort, Antoni Lluís Mesquida, and Antònia Mas. "ISO 31000-based integrated risk management process assessment model for IT organizations". *J. Softw. Evol. Process.* 31.1 (2019). DOI: 10.1002/smr.1984 (cit. on p. 1).

[6] Bob Blakley, Ellen McDermott, and Dan Geer. "Information Security is Information Risk Management". In: *Proceedings of the 2001 Workshop on New Security Paradigms*. NSPW '01. Cloudcroft, New Mexico: Association for Computing Machinery, 2001, pp. 97–104. DOI: 10.1145/508171.508187 (cit. on p. 5).

[7] Mark Burdon, Jodie Siganto, and Lizzie Coles-Kemp. "The regulatory challenges of Australian information security practice". *Comput. Law Secur. Rev.* 32.4 (2016), pp. 623–633. DOI: 10.1016/j.clsr.2016.05.004 (cit. on p. 1).

[8] Pavel Castka and Charles J. Corbett. "Management Systems Standards: Diffusion, Impact and Governance of ISO 9000, ISO 14000, and Other Management Standards". *Found. Trends Technol. Inf. Oper. Manag.* 7.3-4 (2015), pp. 161–379. DOI: 10.1561/0200000042 (cit. on p. 1).

[9] Huseyin Cavusoglu, Birendra Mishra, and Srinivasan Raghunathan. "A Model for Evaluating IT Security Investments". *Commun. ACM* 47.7 (July 2004), pp. 87–92. DOI: 10.1145/1005817.1005828 (cit. on p. 6).

[10] Dorothy E. Denning and Peter J. Denning. "Data Security". *ACM Comput. Surv.* 11.3 (Sept. 1979), pp. 227–249. DOI: 10.1145/356778.356782 (cit. on p. 6).

[11] Georges Dionne. "Risk management: History, definition, and critique". *Risk management and insurance review* 16.2 (2013), pp. 147–166 (cit. on p. 5).

[12] Paul Dolan et al. "Influencing behaviour: The mindspace way". *Journal of economic psychology* 33.1 (2012), pp. 264–277. DOI: 10.1016/j.joep.2011.10.009 (cit. on pp. 18, 19).

[13] Amanda Dunkel and Sylvia Meierewert. "Culture standards and their impact on teamwork: An empirical analysis of Austrian, German, Hungarian and Spanish culture differences". eng. *Journal for East European Management Studies* 9.2 (2004), pp. 147–174. URL: https://hdl.handle.net/10419/90196 (cit. on p. 29).

[14] Marta R Durantini et al. "Conceptualizing the influence of social agents of behavior change: A meta-analysis of the effectiveness of HIV-prevention interventionists for different groups." *Psychological bulletin* 132.2 (2006), p. 212. DOI: 10.1037/0033-2909.132.2.212 (cit. on p. 18).

[15] Security Engineering and Risk Management Group. *NIST Releases SP 800-160 Vol. 2: Developing Cyber Resilient Systems A Systems Security Engineering Approach*. Standard. Gaithersburg: National Institute of Standards and Technology, 2019 (cit. on p. 6).

[16] European Parliament. *Cybersecurity Act*. 2019. URL: https://eur-lex.europa.eu/eli/dir/2019/881/oj (cit. on p. 1).

[17] European Parliament. *Directive*. URL: https://eur-lex.europa.eu/EN/legal-content/glossary/directive.html (cit. on p. 9).

[18] European Parliament. *General Data Protection Regulation*. 2016. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (cit. on pp. 1, 8).

[19] European Parliament. *NIS Directive*. 2022. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj (cit. on p. 1).

[20] European Parliament. *Regulation*. URL: https://eur-lex.europa.eu/EN/legal-content/glossary/regulation.html (cit. on p. 8).

[21] Federal Office for Information Security. *BSI-Standard 200-3: Risk Analysis based on IT-Grundschutz*. 2018. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2003_en_pdf.html?nn=908032 (cit. on p. 11).

[22] Michael GleiSSner et al. "IT Security of Cloud Services and IoT Devices in Healthcare". *CLOUD COMPUTING 2021* (2021), p. 10 (cit. on p. 5).

[23] Sarang Hashemi et al. "Sharpening clinical decision support alert and reminder designs with MINDSPACE: A systematic review". *International Journal of Medical Informatics* 181 (2024), p. 105276. DOI: https://doi.org/10.1016/j.ijmedinf.2023.105276 (cit. on p. 15).

[24] Ajla erimagi Hasibovi, Anel Tanovi, and Aida Granulo. "The importance of ITIL4 adoption for IT service management in insurance companies". In: *2023 46th MIPRO ICT and Electronics Convention (MIPRO)*. 2023, pp. 1341–1346. DOI: 10.23919/MIPRO57284.2023.10159950 (cit. on p. 13).

[25] International Organization for Standardization. *ISO 27000 - Information technology Security techniques Information security management systems Overview and vocabulary*. 2014. URL: https://www.iso.org/standard/27000 (cit. on p. 8).

[26] International Organization for Standardization. *ISO 27001 - Information security management systems*. 2022. URL: https://www.iso.org/standard/27001 (cit. on pp. 1, 8, 9).

[27] International Organization for Standardization. *ISO 27001 - Information technology Security techniques Information security risk management*. 2018. URL: https://www.iso.org/standard/75281.html (cit. on pp. 1, 10).

[28] International Organization for Standardization. *ISO 31000 - Risk management*. 2018. URL: https://www.iso.org/iso-31000-risk-management.html (cit. on pp. 1, 10, 11).

[29] International Organization for Standardization. *ISO 9000 - Quality management systems*. 2015. URL: https://www.iso.org/standard/45481.html (cit. on pp. 1, 13).

[30] International Organization for Standardization. *ISO Directives*. URL: https://www.iso.org/sites/directives/current/consolidated/index.html (cit. on p. 8).

[31] International Organization for Standardization. *ISO Guides*. URL: https://www.iso.org/iso-guides.html (cit. on p. 8).

[32] International Organization for Standardization. *Risk management Vocabulary*. 2009. URL: https://www.iso.org/standard/44651.html (cit. on pp. 9, 11).

[33] ISO/IEC JTC 1/SC 27. *Information technology Security techniques Management of information and communications technology security*. Standard. Geneva, CH: International Organization for Standardization, Mar. 2004 (cit. on p. 5).

[34] ISO/IEC JTC 1/SC 27. *Information security, cybersecurity and privacy protection Information security controls*. Standard. Geneva, CH: International Organization for Standardization, Feb. 2022 (cit. on pp. 5, 10).

[35] ISO/IEC JTC 1/SC 27. *Information technology Security techniques Guidelines for cybersecurity*. Standard. Geneva, CH: International Organization for Standardization, Mar. 2012 (cit. on p. 6).

[36] Bojan Jelacic et al. "Security risk assessment-based cloud migration methodology for smart grid OT services". *Acta Polytechnica Hungarica* 17.5 (2020), pp. 113–134 (cit. on p. 5).

[37] Corinne N Johnson. "The benefits fo PDCA". *Quality Progress* 35.5 (2002), p. 120. URL: https://www.proquest.com/openview/6fb24b731a9c0c8bafd90096fd751e76/1?pq-origsite=gscholar&cbl=34671 (cit. on p. 11).

[38] Hollmann Julia, Aletéia Carpes, and Thiago Beuron. "The DaimlerChrysler merger a cultural mismatch?" *Revista de Administração da UFSM* 3 (Jan. 2011). DOI: 10.5902/198346592506 (cit. on p. 1).

[39] Dennis-Kenji Kipker. "EU Cybersecurity Act and Certification Schemes: an up-to-date progress report". *Datenschutz und Datensicherheit* 44.6 (2020), pp. 390–392. DOI: 10.1007/s11623-020-1290-4 (cit. on p. 1).

[40] Alexander Klimburg. *National cyber security framework manual*. Tallinn: NATO Cooperative Cyber Defense Center of Excellence, 2012 (cit. on p. 7).

[41] Nobuyuki Kobayashi et al. "A Proposal of Information Security Policy Agreement Method for Merger and Acquisition Using Assurance Case and ISO 27001". In: *2019 8th International Congress on Advanced Applied Informatics (IIAI-AAI)*. 2019, pp. 727–733. DOI: 10.1109/IIAI-AAI.2019.00150 (cit. on p. 15).

[42] Yevhenii Kurii and Ivan Opirskyy. "Analysis and Comparison of the NIST SP 800-53 and ISO/IEC 27001: 2013". In: *Proceedings of the Cybersecurity Providing in Information and Telecommunication Systems, CPITS 2022, co-located with International Conference on Problems of Infocommunications. Science and Technology (PICST 2022), Kyiv, Ukraine, October 13, 2022 (online)*. Ed. by Volodymyr Sokolov et al. Vol. 3288. CEUR Workshop Proceedings. CEUR-WS.org, 2022, pp. 21–32. URL: https://ceur-ws.org/Vol-3288/paper3.pdf (cit. on p. 1).

[43] Paul Lackner. "Security thoughts on modern software development". MA thesis. UAS St. Pölten, 2021 (cit. on p. 6).

[44] B.W. Lampson. "Computer security in the real world". *Computer* 37.6 (2004), pp. 37–46. DOI: 10.1109/MC.2004.17 (cit. on p. 5).

[45] Carl E Landwehr. "Computer security". *International journal of information security* 1.1 (2001), pp. 3–13. DOI: 10.1007/s102070100003 (cit. on pp. 4, 5).

[46] Ralph Langner. "Stuxnet: Dissecting a cyberwarfare weapon". *IEEE Security & Privacy* 9.3 (2011), pp. 49–51 (cit. on p. 6).

[47] Benedikt Lebek et al. "Information security awareness and behavior: a theory-based literature review". *Management Research Review* (2014) (cit. on p. 5).

[48] Sergio Francisco Sargo Ferreira Lopes. "The importance of the ITIL framework in managing Information and Communication Technology services" (2021). DOI: 10.22161/ijaers.85.35 (cit. on p. 13).

[49] MacMillan Dictionary. *Cyber*. URL: https://www.macmillandictionary.com/dictionary/british/cyber (cit. on p. 6).

[50] Finbarr Murphy Martin Cunneen Martin Mullins and Seán Gaines. "Artificial Driving Intelligence and Moral Agency: Examining the Decision Ontology of Unavoidable Road Traffic Accidents through the Prism of the Trolley Dilemma". *Applied Artificial Intelligence* 33.3 (2019), pp. 267–293. DOI: 10.1080/08839514.2018.1560124 (cit. on p. 4).

[51] Herbert J. Mattord and Michael E. Whitman. "Regulatory Compliance in Information Technology and Information Security". In: *Reaching New Heights. 13th Americas Conference on Information Systems, AMCIS 2007, Keystone, Colorado, USA, August 9-12, 2007*. Ed. by John A. Hoxmeier and Stephen C. Hayne. Association for Information Systems, 2007, p. 357. URL: http://aisel.aisnet.org/amcis2007/357 (cit. on p. 1).

[52] Ines Meriah and Latifa Ben Arfa Rabai. "Comparative Study of Ontologies Based ISO 27000 Series Security Standards". In: *The 10th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2019) / The 9th International Conference on Current and Future Trends of Information and Communication Technologies in Healthcare (ICTH-2019) / Affiliated Workshops, Coimbra, Portugal, November 4-7, 2019*. Ed. by Elhadi M. Shakshuki, Ansar-Ul-Haque Yasar, and Haroon Malik. Vol. 160. Procedia Computer Science. Elsevier, 2019, pp. 85–92. DOI: 10.1016/j.procs.2019.09.447 (cit. on p. 1).

[53] Merriam Webster Dictionary. *Privacy*. URL: https://www.merriam-webster.com/dictionary/privacy (cit. on p. 8).

[54] Merriam Webster Dictionary. *Safety*. URL: https://www.merriam-webster.com/dictionary/Safety (cit. on p. 4).

[55] Ola Aleksandra Michalec et al. "Industry Responses to the European Directive on Security of Network and Information Systems (NIS): Understanding policy implementation practices across critical infrastructures". In: *Sixteenth Symposium on Usable Privacy and Security, SOUPS 2020, August 7-11, 2020*. Ed. by Heather Richter Lipford and Sonia Chiasson. USENIX Association, 2020, pp. 301–317. URL: https://www.usenix.org/conference/soups2020/presentation/michalec (cit. on p. 1).

[56] Kevin D Mitnick and William L Simon. *The art of deception: Controlling the human element of security*. Hoboken: John Wiley & Sons, 2003 (cit. on p. 5).

[57] National Institute of Standards and Technology. *NIST800-53 - Security and Privacy Controls for Information Systems and Organizations*. 2020. URL: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final (cit. on p. 1).

[58] Mike Nimród. "European privacy by design". PhD thesis. Corvinus University of Budapest, Hungary, 2023. URL: https://doktori.hu/index.php?menuid=193%5C&lang=HU%5C&vid=26033 (cit. on p. 8).

[59] Calvin Nobles. "Stress, Burnout, and Security Fatigue in Cybersecurity: A Human Factors Problem". *HOLISTICA Journal of Business and Public Administration* 13.1 (2022), pp. 49–72. DOI: doi:10.2478/hjbpa-2022-0003 (cit. on pp. 39, 41).

[60] Verónica Pérez-Rosas et al. "Automatic Detection of Fake News". In: *Proceedings of the 27th International Conference on Computational Linguistics, COLING 2018, Santa Fe, New Mexico, USA, August 20-26, 2018*. Ed. by Emily M. Bender, Leon Derczynski, and Pierre Isabelle. Santa Fe: Association for Computational Linguistics, 2018, pp. 3391–3401. URL: https://aclanthology.org/C18-1287/ (cit. on p. 6).

[61] Andreas T. Schmidt and Bart Engelen. "The ethics of nudging: An overview". *Philosophy Compass* 15.4 (2020), e12658. DOI: https://doi.org/10.1111/phc3.12658. eprint: https://compass.onlinelibrary.wiley.com/doi/pdf/10.1111/phc3.12658 (cit. on p. 19).

[62] Adam Shostack. "Experiences Threat Modeling at Microsoft" (2008). URL: https://adam.shostack.org/modsec08/Shostack-ModSec08-Experiences-Threat-Modeling-At-Microsoft.pdf (cit. on p. 12).

[63] Mikko T. Siponen, Seppo Pahnila, and M. Adam Mahmood. "A New Model for Understanding Users' IS Security Compliance". In: *Pacific Asia Conference on Information Systems, PACIS 2006, Kuala Lumpur, Malaysia, July 6-9, 2006*. Kuala Lumpur: AISeL, 2006, p. 48. URL: http://aisel.aisnet.org/pacis2006/48 (cit. on p. 5).

[64] Hadley Stevens Smith et al. "A review of the MINDSPACE framework for nudging health promotion during early stages of the COVID-19 Pandemic". *Population health management* 25.4 (2022), pp. 487–500. DOI: 10.1089/pop.2021.0269 (cit. on p. 15).

[65] Michael L Smith, James Erwin, and Sandra Diaferio. "Role & responsibility charting (RACI)". In: *Project Management Forum (PMForum)*. Vol. 5. 2005. URL: https://www.workfront.com/sites/default/files/imported/pdfs/raci_r_web3_1.pdf (cit. on p. 12).

[66] Rossouw von Solms. "Information security management (3): the Code of Practice for Information Security Management (BS 7799)". *Inf. Manag. Comput. Secur.* 6.5 (1998), pp. 224–225. DOI: 10.1108/09685229810240158 (cit. on p. 5).

[67] Igli Tashi. "Regulatory Compliance and Information Security Assurance". In: *Proceedings of the The Forth International Conference on Availability, Reliability and Security, ARES 2009, March 16-19, 2009, Fukuoka, Japan*. IEEE Computer Society, 2009, pp. 670–674. DOI: 10.1109/ARES.2009.29 (cit. on p. 1).

[68] Yeshwanth Valaboju. "A Comprehensive Study On Iot Architectures And Iot Security". *Parishodh Journal* 8 (2019) (cit. on p. 6).

[69] Rossouw Von Solms and Johan Van Niekerk. "From information security to cyber security". *computers & security* 38 (2013), pp. 97–102. DOI: 10.1016/j.cose.2013.04.004 (cit. on pp. 5–7).

[70] Michael E Whitman and Herbert J Mattord. *Principles of information security*. Boston: Cengage learning, 2011 (cit. on p. 5).

[71] Richmond Y. Wong, Andrew Chong, and R. Cooper Aspegren. "Privacy Legislation as Business Risks: How GDPR and CCPA are Represented in Technology Companies' Investment Risk Disclosures". *Proc. ACM Hum. Comput. Interact.* 7.CSCW1 (2023), pp. 1–26. DOI: 10.1145/3579515 (cit. on p. 1).

[72] Charles Cresson Wood. "Why information security is now multi-disciplinary, multi-departmental, and multi-organizational in nature". *Computer Fraud & Security* 2004.1 (2004), pp. 16–17 (cit. on p. 5).

Online sources

[73] Axelos. *What is ITIL*. URL: https://www.axelos.com/certifications/itil-service-management/what-is-itil/ (visited on 01/04/2024) (cit. on p. 13).

[74] ISACA. *What is CMMI*. URL: https://www.isaca.org/enterprise/cmmi-performance-solutions (visited on 02/03/2024) (cit. on p. 14).

[75] ISACA. *What is COBIT*. URL: https://www.isaca.org/resources/cobit (visited on 01/04/2024) (cit. on p. 13).

[76] ISO. *What to expect from a Redline*. URL: https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/iso_10123_redline_version_sample.pdf (visited on 02/11/2024) (cit. on p. 22).

[77] Tom Mannerud. *The Security Awareness Cycle*. URL: https://web.archive.org/web/20210911204341/https://www.mannerud.org/tom-andreas/security-awareness/the-security-awareness-cycle/ (visited on 12/10/2023) (cit. on pp. 17, 18).

[78] Microsoft. *The STRIDE Threat Model*. 2009. URL: https://learn.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20) (visited on 02/11/2024) (cit. on p. 12).