Information Security

SecDT-Framework

Combining Design Thinking with Information Security and Data Protection

Diplomarbeit

zur Erlangung des akademischen Grades

Diplom-Ingenieur/in

eingereicht von

Lukas König

IS191836

im Rahmen des

Studienganges Information Security an der Fachhochschule St. Pölten

Betreuung

Betreuer/in: FH-Prof. Dr. Simon Tjoa

Mitwirkung:

St. Pölten, 31st August 2021

(Unterschrift Verfasser/in) (Unterschrift Betreuer/in)

*

Fachhochschule St. Pölten GmbH, Matthias Corvinus-Straße 15, A-3100 St. Pölten,T: +43 (2742) 313 228, F: +43 (2742) 313 228-339, E:office@fhstp.ac.at, I:www.fhstp.ac.at

Ehrenwörtliche Erklärung

Ich versichere, dass

- ich diese Diplomarbeit selbständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich sonst keiner unerlaubten Hilfe bedient habe.
- ich dieses Diplomarbeitsthema bisher weder im Inland noch im Ausland einem Begutachter/einer Begutachterin zur Beurteilung oder in irgendeiner Form als Prüfungsarbeit vorgelegt habe.
- diese Arbeit mit der vom Begutachter/von der Begutachterin beurteilten Arbeit übereinstimmt.

Der Studierende/Absolvent räumt der FH St. Pölten das Recht ein, die Diplomarbeit für Lehre- und Forschungstätigkeiten zu verwenden und damit zu werben (z.B. bei der Projektevernissage, in Publikationen, auf der Homepage), wobei der Absolvent als Urheber zu nennen ist. Jegliche kommerzielle Verwertung/Nutzung bedarf einer weiteren Vereinbarung zwischen dem Studierenden/Absolventen und der FH St. Pölten.

Ort, Datum *Unterschrift*

Kurzfassung

Es ist allseits bekannt, dass der *Faktor Mensch* eines der größten Probleme und Verursacher von vielen Sicherheits-Vorfällen in Organisationen ist. Die Situation hat sich über die letzten Jahre, zum Teil auch pandemiebedingt, zum Schlechteren gewendet. Traditionell wird versucht mit Schulungen und Training solche Lücken zu schließen, doch die Effekte lassen oftmals auf sich warten. Diese Diplomarbeit verfolgt einen anderen Ansatz. Die Probleme des Menschen im Umgang mit Cybersicherheit sollen dadurch gelöst werden, indem man auf den Menschen gerichtete Methoden verwendet. So soll Design Thinking mit Informationssicherheit und Datenschutz kombiniert werden, um am Ende ein Framework zum kreativen und menschenfokussierten Umgang mit der Thematik zu erhalten, welches die üblicherweise starren Themen berücksichtigt. Um dieses Ziel zu erreichen werden zuerst die fundamentalen Bausteine der jeweiligen Bereiche ermittelt und untersucht. Anschließend werden sie auf Gemeinsamkeiten hin überprüft. Ein experimentelles SecDT-Framework wird erstellt und an einer Partnerorganisation getestet. Das Experiment hat bestätigt, dass es durchaus möglich ist die in ihrer Natur stark widersprüchlichen Welten des Design Thinking und der Informationssicherheit/Datenschutz zu vereinen, da viele Elemente einen ähnlichen Nutzen haben und somit quer über die Modelle in einer gewissen Art und Weise vorhanden sind. Es kann geschlussfolgert werden, dass ein kreativer Ansatz zur Thematik besonders in einem kreativen Umfeld den Effekt vervielfacht und zugänglicher macht. Somit kann Sicherheit mit relativ überschaubarem Aufwand in alle Ebenen einer Organisation entsprechend den vorhandenen Ressourcen vermittelt werden. Besonders kleinere Organisationen und Start-Ups, in denen das Expertenwissen zur Cybersicherheit oftmals nicht ausreichend vorhanden ist könnten von dem kreativen Ansatz des SecDT-Frameworks profitieren, da es ihnen erlaubt sich mit der Thematik zu befassen und zumindest mit bereits vertrauten Herangehensweisen eine Lösung zu finden.

Abstract

It is well known that the human factor is one of the biggest problems and causes of many security incidents in organizations. The situation has taken a turn for the worse over the last few years, partly due to pandemics. Traditionally, training and classroom activities have been used to close such gaps, but the effects are often slow to materialize. This thesis takes a different approach. The problems of humans in dealing with cybersecurity are to be solved by using methods oriented towards humans. Thus, Design Thinking is to be combined with Information Security and Data Protection in order to ultimately provide a framework for dealing with the topic in a creative and human-centered way that takes into account the usually rigid topics. To achieve this goal, the fundamental building blocks of each area are first identified and examined. They are then assessed for commonalities. An experimental SecDT-Framework is created and tested with a partner organization. The experiment has confirmed that it is entirely possible to unite the worlds of design thinking and information security/data protection, which are strongly contradictory in nature, as many elements have similar utility and thus exist across the models in some capacity. It can be concluded that a creative approach to the subject matter, especially in a creative environment, multiplies the effect and makes it more accessible. Thus, security can be communicated to all levels of an organization with relatively manageable effort according to the resources available. Especially smaller organizations and start-ups, where expert knowledge on cybersecurity is often not sufficiently available, could benefit from the creative approach of the SecDT-Framework, as it allows them to engage with the topic and at least find a solution with already familiar approaches.

Contents

Part I.

Introduction and General Information

1. Introduction

In a recent report [1], the Federal Criminal Police Office recorded a steady increase of criminal online activities in Austria over the last years, with a growth of almost 17% in 2018 compared to the previous year. Not only is this a dangerous development as life becomes gradually more digitised, the risk is exceedingly high during a global pandemic that forces an unforeseen amount of people to work from their own homes with private devices instead of enjoying the full perimeter protection of their companies, as we experience during COVID-19. Additionally, [2] confirms this trend with statistical developments in the United Kingdom. The Office of National Statistics and the Business Crime Survey make it apparent that this number is exorbitantly high and will increase steadily. The often cited most vulnerable element in all cybersecurity defences is the human operator. To put this into perspective, the estimated cost caused by fraudulent online activities amounts to a £193 billion in 2016.

These numbers suggest that the measures to secure the human as part of the cyber defences are either insufficient or heading in a wrong direction. Adding to the already less than perfect situation, a survey conducted by Deloitte about cybersecurity and it's development during COVID-19 in 2020 [3] underline that the overall security levels of data and IT systems decreased in more than 20% of participating companies. Even more disturbing is that more than 80% of the respondents stated that they do not have a plan of what to do in case of a cyber attack. Furthermore, almost half of the participants stated that they experienced an increase of privately owned devices being used for professional purposes and almost two thirds confirm that risks emanating from human behaviour became an even more concerning factor.

As pointed out in [2], there are some major problems regarding what information security should be and how it is actually executed. The concept of a malicious insider is already well known, understood and studied, similarly the different factors and prerequisites that lead to the creation of one. That's not to say that a successful attack or exploit must include only malicious actors. The so called *accidental insider* is just as likely to cause damage and pose a threat to information security. These threats emerge from a lack of awareness, knowledge, concern or proficiency in managing data and devices. These claims are backed up in [4], where a conducted survey found that almost all participants do not see information security as their field of duty in any form and the majority would not even be able to react or uphold the defences in case of a cyber emergency because they see themselves unfit and not engaged to the matter, with some

even claiming that information security is an exclusive problem of machines and computers. This is not true however, as human actions and the human factor are a pillar of every grand strategy on information security and cyber defences [5].

While the overall number of fraudulent online activities increases, it's composition started to change recently. Attacks directed towards machines and technical systems are less popular due to increasing technological advances and security measures. Concurrently, the number of attacks targeting the human element increased in equal measure, clearly indicating the preferred weakest link for an attacker [1]. Additionally, the 2020 Sophos Threat Report [6] points out that technologies such as AI and machine learning are an additional hurdle, as they can be used to trick humans with increasingly legitimate appearing generated content and deepfakes. The problematic nature grows alongside technological and psychological advances.

Both [4] and [5] underline the importance of tearing down the barriers between human operators and their devices. Information security education and the importance of actively taking part must be portrayed in a way that help the individuals to understand what risks they are dealing with and how they are influencing a possible outcome. Cybersecurity practices are tremendously lacking empathy and human-centered design approaches for information security systems. The field of information security will profit from advances that incorporate and integrate the individual into cyber defence systems by focusing on human perception and awareness.

Another major factor of human-centered information security is trust. In [7], the authors state that trust is essential, not only on a regular work basis where the users have to be trusted to not conduct any information security offences, but also for risk assessment. Whether human risk gets classified as positive or negative is dependant on the level of trust in their abilities to do the right thing in the right situation. There are several factors that impact trust (e.g. education and training, situational awareness, experience, etc.) which in turn can be influenced by according measures. Oltramari et al. [8] point out that trust in machines and devices is an integral part for a functioning man-machine interaction, especially for individuals that are not familiar with technology. In that context, trust can be built by showing consistency and providing a user experience to give the feeling of being in good hands. Such an experience is usually achieved by human/user-centred design methods. Furthermore, in the provided *Trust Framework of Human Factors in Cyber Security* the authors emphasize and illustrate once more how various factors, both internal and external, can influence trust.

Since the human factor is such a fundamental part for effective information security, providing a positive experience of the often obscure practices and policies used for cyber security must be imperative. There are several ways of achieving this goal. The approach used in this thesis is utilising Design Thinking, its principles, tools and methods to implement information security processes and overcome its human-centred problems.

1.1. Scope of the thesis

For companies of varying sizes and industries, the topic of information security and data protection is valued differently. To give an example, a software development company has its employees working with computers all day. A restaurant or hotel does not see technology in the same light. Nonetheless, both of them have to secure their data and information. The effectiveness of such a safeguarding is directly dependent on the technological literacy of the employees. The scope of this thesis therefore lies on providing a new way of thinking about a concept for cyber security practices and their approaches to information security and data protection. Depending on the type of enterprise, a Design Thinking approach for information security and data protection might be more in line with already existing processes and environments within a company. Especially businesses that are already familiar with the ideas of Design Thinking could potentially benefit the most from using such methods.
This thesis aims at creating a guiding framework to conceptualize information security and data protection by using Design Thinking methods, principles and tools. Creating such a framework could take an unpredictable amount of time which could lead to unexpected delays in the procedure of this thesis. Furthermore, as Design Thinking is used as a mean of conveying the ideas of information security and data protection, being familiar with Design Thinking will be an advantage, but should not be a requirement.
To summarise, the scope of this thesis is to create a framework that utilizes Design Thinking principles, methods and tools to achieve the overall objective of securing a company and being compliant to requirements of according laws and standardisation targets by supporting the conceptualization of information security and data protection within a business.

1.2. Research Problem and Research Question

This thesis aims at creating a framework and combining elements which seem to be contrary at first with information security and data protection being a strongly structured and regulated approach, whereas Design Thinking is very fluid and variable. Therefore, the research problems are the intricacies and

challenges of combining Design Thinking with information security and data protection. This challenge will be the main obstacle to overcome. The intention of the presented framework is to help companies conceptualize information security and data protection with the alternative approach of using Design Thinking. Ensuring sophistication on all levels could push boundaries.
The overall problem can be divided into a number of smaller and more specific problems:

- Definitions of and work on Design Thinking, information security and data protection.
- Creation and proposal of a valid model/framework that combines Design Thinking with information security and data protection.
- Consideration of standardisation and legal requirements such as ISO 27001, GDPR, and NIS-Regulation.
- Generation of value for potential users of this proposed framework.

In this thesis, the identified problems shall be answered with according solutions to the best of the author's abilities. To achieve this, a set of research questions, deriving from the stated problems, are formulated to provide guidance during the research. The preliminary task is to establish requirements and elements of Design Thinking, information security and data protection. After that, the following questions shall be answered:

- How can a framework combining these elements be arranged, considering regulatory and normative requirements, as well as Design Thinking principles?
- How is such a framework received by companies?

1.3. Contribution & Structure

The main contribution of this thesis is the creation of the *SecDT-Framework*, which combines Design Thinking with information security and data protection. An experiment of one test iteration to assess the framework's impact on and usefulness for organizations will be conducted. The insights gathered during the experiment and in an interview afterwards will form the basis for an evaluation and discussion of the framework.
The remainder of this thesis consists of two additional parts. Part II analyzes the theory behind Design Thinking, information security and data protection, their principles, methods and tools, as well as defining what is necessary to include based on legal requirements. This part will therefore cover the following parts in its sections:

- An introduction to Design Thinking;
- An overview of common Design Thinking tools and techniques;
- An overview of Design Thinking processes and process models;
- An overview of the fundamentals of information security;
- An outline about the legal situation of data protection in Austria.

Part III will then be used for the creation of the framework itself. This framework will be built based on the research of the previous part and is set to provide an alternative way for organizations to introduce these topics in their organization or to improve on existing systems. The framework will be tested with a participating partner organization. The effectiveness and quality of the framework will be evaluated and analyzed to detect areas for possible future improvement. This part will be structured as follows:

- Considerations on possibilities for harmonization of Design Thinking with information security and data protection and its incompatibilities;
- Creation of the framework with an experimental iteration;
- Evaluation and discussion of the SecDT-Framework;
- Conclusion.

The annex of this thesis will include the interview with the partner organization, which will take place shortly after the experiment has ended. Additionally, the results of the workshop will be annexed as well, to provide the content in a form that is more legible as these records will not have to be compacted.

2. Methodology & Background

This chapter outlines the methodology of the thesis and presents background information and related work. It serves as a guideline for the overall structure of what be included and provides fundamental information.

2.1. Methodology

As already mentioned before, this thesis can generally be divided into two major parts after regarding its main content. The first of these parts will focus on the theory and theoretical constructs of Design Thinking, information security and data protection. Each of these will be further divided into definitions, tools and methods, and existing frameworks, depending on the context and the available information. The objective of this elaboration is to list and identify essential and relevant factors in each category, which will be needed for the creation of a basic Design Thinking framework with which information security and data protection can be introduced to companies, that considers the research questions. Besides regular literature on the matter, both the GDPR and the ISO 27001 will be dissected into their most relevant pieces.

The second part will be the creation of a general framework. The previous theoretical research in the first part will form the foundation on which the framework is built. The challenge here is to find a way to combine usually rigid elements like the heavily standardised processes in the fields of information security and data protection, which usually are limited by severe regulations and laws, with Design Thinking. Design Thinking itself has a wholly different approach on solving problems and with that, a certain set of benefits over traditional problem solving methods. The key is to leverage these benefits and use them to get the most out of both worlds.

Once such a framework is created, it will be tested and evaluated with the help of a participating company that is interested in introducing the subjects on hand into their business.

With the research work conducted in these chapters, the end result shall answer all of the research ques-

tions and provide insight on the matter which can then be used to refine the framework even more or make further adaptions to it for a more delicate and specialised field of use, as this thesis focuses on delivering a generalized approach.

2.2. Background & Related Work

This section covers work that is of relevance for this thesis that need further explanation or background information, especially Design Thinking itself, which is not overly present in the field of information security and therefore might be unfamiliar to readers of this thesis. Not only are there papers with similar ideas, i.e. combining Design Thinking and software development, but also general approaches on Privacy/Security by Design or Design Thinking. Each of these sources of this background research will be shortly explained and clustered into groups according to their areas of research to provide a better overview of these sources.

Design Thinking

The authors of [9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22] describe what Design Thinking means and what issue it is supposed to solve and the close ties of Design Thinking and innovation. They describe Design Thinking not only as a way of solving problems, but an entirely different school of thought that is used to drive innovation by need-oriented problem solving that focuses on the people involved. It is also a mindset that follows a set of principles and uses various processes. In [11], the authors also list the differences between traditional business practices and Design Thinking. Additionally to fundamental definitions and explanations, the authors of [12] lay out guidelines on how to use Design Thinking across all business processes, which are aimed towards entrepreneurs and small businesses.

Design Thinking processes, tools and toolkits, and formulas for creative brainstorming are described in [9, 10, 11, 13, 14, 16, 23, 24, 25, 17, 19, 26, 20, 21]. These processes are essential to the overall success of the application of Design Thinking and will be discussed in more detail in the following chapters.

In the field of information security, there is often times a mention of metrics and the importance of measuring progress and success to support continuous improvement. In [12, 27], the authors provide a set of metrics to evaluate Design Thinking practices so these processes too can be gradually improved and tailored towards maximum success. The impact of metrics for Design Thinking is also discussed in [27]. About the effectiveness, there are two important mentions. One being that depending of the cultural understanding and background of both the ones designing and the persons having to use the designed

product, it can lead to misunderstandings based on varying cultural assumptions [28]. Additionally, when something gets designed in theory, it can still yield unexpected results in practice [29].

It is described in [14], that Design Thinking is also an important tool for risk mitigation and a general reduction of occurrence probability of risks. It is argued that by working closely together with the needs of the individual (customer), the final product will be much closer to what is actually needed, rather than rigid products that blindly follow a set of criteria without feedback along the way. Producing or developing something should always be an approximation to the needs of the humans involved.

Design Thinking Approaches in the field of Software Engineering and IT-Innovation

Design Thinking as a different school of thought is seen as a radical way for innovation instead of incremental improvement that is much more typical in the field of IT by the authors of [9]. They state *SAP HANA* as a prime example for that, which is supported by [20].

Design Thinking is often seen as a crucial enabler for any form of software or information system development because of the human-computer-interaction. Various projects and research in that direction was carried out in the past, as mentioned by [10]. The same argument is reinforced by i.e. [16, 17, 30, 31, 18, 26], where empathy and human understanding is moved to the center, especially in agile work modes. Adding to that, [32] states that the *human* part of a human-computer-interaction cannot be dealt with by looking at a problem from a purely technical perspective, as it traditionally tends to be. The focus on the user becomes even more apparent when looking at it from a *service Design Thinking* perspective, where processes are crafted to provide the best possible user experience [21]

In [17], it is described that Design Thinking is not simply something that can be used to stimulate innovation, but is seen as a very essential skill-set of a modern software developer. Human-centered development is highlighted as a key factor in providing the best possible experience for end users of a software. Perception of what humans see and feel during such an interaction should be the focus of any modern development process. Furthermore, in their analysis they state that the use of Design Thinking in the process of software development is one of the most valuable assets. Others have recognized the benefits of utilizing Design Thinking and started including it into software development classes or frameworks [19, 18, 26].

Design Thinking combinations in other realms

Design Thinking Research

Design Thinking research is the focus of the cooperation between the *Hasso Plattner Institute for Soft-*

ware Systems Engineering and the *Center for Design Research* at Stanford University. Various articles are joined together by the editorial in [33, 34, 35]. Their overall research on Design Thinking subscribes to the idea that in any form of engineering or information system, ultimately everything that is done comes down to the human nature and human actions. Therefore, it is vital for innovation and success of a modern company to adapt to these. Empathy and the influence on the individual is seen as a centerpiece of all Design Thinking efforts. Additionally, there is a strong focus on team collaboration and the positive effects of proper teamwork in reaching certain objectives.

Design Thinking for Startups

Many authors write about the importance of Design Thinking for start-ups and small enterprises. These range from entrepreneurial advice and teamwork strategies to building entire business models around the idea of Design Thinking [36, 12, 33, 34, 15, 26].

Information Security

For most readers of this thesis, information security will most likely be something that they are already familiar with. However, there are characteristic terms that should be known and understood by everyone, since they play a crucial role in information security. Therefore, the most relevant terminology and the meaning behind these words will be highlighted here shortly.

The three most commonly used words in conjunction with information security are without a doubt *Confidentiality, Integrity* and *Availability*. According to the definitions of [37], they are equally as important as the meaning of *information* itself and pillars of any information security efforts. In this work by the National Institute of Standards and Technology, they define the meaning of these words as the following:

- Confidentiality - Preserving authorized restrictions on information access and disclosure.
- Integrity - Guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity
- Availability - Ensuring timely and reliable access to and use of information.

Furthermore, they go on and differentiate between data integrity and systems integrity, which try to achieve the same objective on their respective targets. This trinity, often times called the CIA of information security, forms the basis of any information security endeavor.

As rightfully pointed out by [38, 39, 40], there are more (sub)-factors that need to be considered when dealing with information security. Some of these factors include *authenticity, cryptography, dependability, trust, correctness* and *responsibility*, to name a few.

The standard ISO/IEC 27001 [41] by the *International Organization for Standardization* has become the information security baseline in many sectors. Building and maintaining an information security management system has become a crucial activity for protecting companies against digital threats. According to a survey [42], there were about 40,000 certified companies in 2017 with an increase of 19% to the previous year. This shows that the need for being certified is increasing. The same survey was conducted in 2019 [43] and revealed that now almost 69,000 sites received an ISO/IEC 27001 certification.

The term *security by design* is often used in conjunction with software development and information security. It is however not related to Design Thinking itself. The objective of security by design is to design a system in a way that makes it secure from the beginning [44, 45, 46]. This means that a higher need for security is attributed to a system and it is ensured that a number of security requirements are included in the process of creation of the system. However, it is not the same as Design Thinking in software/systems engineering.

Data Protection

When the *General Data Protection Regulation* [47] came into force, many companies were not prepared to comply to the new rules. Especially small- and medium-sized enterprises were hit hard by the requirements, as they often struggle with according resources or know-how[48, 49].

One term that gained traction very quickly is *privacy by design*. What this means is that privacy should be included in the development process from the very beginning [50, 51, 52, 53, 54]. The seven principles of privacy by design are outlined in [55]. In addition to these, there are new protective objectives that arose [56]. Similarly to security by design, privacy by design tries to achieve an entire different set of objectives than Design Thinking.

However, in [57], the authors have shown that Design Thinking can be used to ease the implementation and reduce the challenges of all tasks required for successful privacy by design. Not only that, but using Design Thinking for such an implementation could even yield better results, because of socio-technological contexts that would otherwise not be detected from a purely technological point of view.

Human-centric Information Security

As already pointed out in the introduction, the human factor is an integral part of information security. The interaction between humans and devices of information systems of a cyberspace is crucial when it comes to understanding human behaviour, needs and especially security risks [58]. Focusing on and securing humans should not be seen any lesser than implementing technical security measures on an information system. Especially when it comes to operating and securing a system, it is still a human doing the work. The importance of the human socio-cognitive behaviour within any system is also highlighted

by [59]. Closely entangled to this socio-cognitive behaviour is the term *security awareness*. The authors go on and argue that specifically this security awareness is key in bringing cyber defences to the next level.

This lack of human-centric cyber security is further explained in [60], where the authors point out reasons for why current efforts are insufficient. Especially in the age of digital transformation. Regard for the individual is seldom considered in the field of cyber security. People are often seen as homogeneous collectives, but it could not be further from the truth. The way someone deals with information and information systems on the individual level requires a lot more focused work than it currently receives. Nowadays, social media is enormously influential and the data and information shared on such platforms, as well as the importance of such places for ideological and cultural exchange reaches intangible levels. This reliance on digital technologies on the individual level requires sufficient awareness and fitting concepts for information security. With the dawn of smart homes and IoT, not only the amount of devices connected to the internet increased, but also the number of attack surfaces and patterns [61]. With the evolution of technology, human habits changed as well. Security and privacy are deeply rooted factors of the *human factor for cybersecurity*. Considering the individual for what he or she is can massively improve our understanding of how we approach issues if cybersecurity.

Of course, training the broad mass of citizens is hardly a viable strategy. But companies around the globe have introduced their own methods and programs of training and educating their staff to become more aware of digital threats and pitfalls [62]. This becomes especially viable and even a necessity during our time of ever increasing quantities of laws and regulations that require certain levels of cyber security for a company to be compliant. But the authors rightfully point out that information security efforts should not be about meeting requirements, but rather focus on nurturing an environment where a security culture can flourish. By ”securing” the human element, compliance will find its way automatically.

The conflict between Design Thinking and Information Systems

The authors of [22] point out that there has been an ongoing effort to try and combine theories and methods of Design Thinking with information systems themselves, but the manifold reasoning that is a fundamental part of design and Design Thinking has not been authentically simulated by an information system so far. The combination of these two worlds have never been an easy task. The focus of their work however is an evaluation of architectural Design Thinking that is supported by information systems and not the use of Design Thinking to build information systems.

Part II.

Design Thinking, Information Security and Data Protection

3. Design Thinking Foundation

Since this thesis aims at combining Design Thinking with information security and data protection, it is first needed to take a closer look at its fundamentals. This chapter will explain and discuss what is needed to understand and use Design Thinking accordingly to the scope and aims of this thesis. Furthermore, most readers coming from the field of information security and data protections are most likely not familiar with terms and ideas from the Design Thinking universe.

3.1. Design Thinking Definitions

Pauwels et al. [22] emphasise that there are multiple varying definitions for Design Thinking with some authors going even so far as place *design knowledge* at the same level as art knowledge or science knowledge. Therefore, the first step towards understanding Design Thinking is to have a proper and especially unified definition of what it actually means. This section will analyse and evaluate a number of available definitions and then conclude which definition will be used as a working definition. This definition will be used for orientation for both, the readers and the work itself.

Meinel et al. defined Design Thinking as a ”thinking and labour culture” that is meant to satisfy human and societal needs through innovation by ”expanding views to understand what humans actually need” [9]. They also call for a multidisciplinary and cooperative approach that is following trusted methods from the design world to trigger innovative breakthroughs.

The Institute of Information Management of the University of St. Gallen focuses on Design Thinking in the context of teaching and information systems. They state a number of definitions, one of them is a reference to the CEO of the innovation consulting company IDEO, Tim Brown. According to him, Design Thinking is a ”discipline that uses the designer’s sensibility and methods to match people’s needs with what is technologically feasible and what a viable business strategy can convert into customer value and market opportunity” [10]. The other definition, referencing Dave Kelly, states that Design Thinking is rather ”a way of finding human needs and creating new solutions using the tools and mindsets of design practitioners”. As the authors correctly point out, it becomes apparent that the human factor

and technological abilities play a vital role in Design Thinking. Where these two definitions contrast themselves is the focus on market opportunity and the involvement with business strategy, which does make sense considering that as a company offering innovation consulting, there needs to be a relevance for the market.

In [11], the authors list a number of differing definitions that they encountered during their research on the matter. Their findings are then pooled into one single definition that encompasses the most important aspects according to their work. To them, Design Thinking means ”finding new solutions to existing problems” with the most important feature being the ”focus on the user and a subsequent positive effect for them”. Furthermore, they mention a Design Thinking process on the same level. This process should be iterative, structured and multidisciplinary. The same idea is revisited in [15].

The authors of [12] point out that design thinking is a skill set that should be used in all industries, as it is an immensely valuable asset to any business. They also elaborate that it might be overwhelming and confusing when someone first starts to actively use Design Thinking, as exploration and non-linear approaches are basically a given. According to them, Design Thinking is an ”exploratory approach to problem solving”, a mindset so to speak, in which thought processes of both worlds, the creative field and the traditional systematic and analytical approach, are combined and balanced into one iterative process.

According to [14], Design Thinking means to ”find solutions” that are able to ”satisfy needs and please the customer”. It is a way of thinking to identify and solve problems by testing possible solutions until something new can be provided. To them, Design Thinking makes it possible to fulfil the needs and withes of customers more accurately and simultaneously reduces the risk of investment and uncertainties.

In [16], the authors state that Design Thinking is the way designers think and work when they come up with solutions for problems of customers while progressing through a design process. The importance of design itself is highlighted, although acknowledging that the understanding of design itself varies depending on its field of use.

In the context of using Design Thinking for software development, [17] defines it as a way of finding innovative solutions to existing problems by using a ”systematic human-centred approach”. This approach consists of the three phases of inspiration, ideation and implementation. What Design Thinking is meant to achieve is satisfying the needs of users by using the Design Thinking mindset for innovation.

Design Thinking as a mindset evolving from the practical application of product design is discussed in [19]. This shows that it is not an immovable object and will change based on its environmental influences and especially needs and requirements. The current form of Design Thinking is defines as a way of thinking that uses innovative ideas to overcome problems with a strong focus on humans and empathy.

A definition of Design Thinking given by the *Interaction Design Foundation* can be summarised as a mindset and way of working with a toolbox aiming at redefining identified problems of users so that solutions can be found that would not become apparent in a traditional thinking and working environment [63]. It is done in an interactive process that is split into several phases.

As clearly visible with such a plethora of slightly varying definitions of what Design Thinking actually is, it illustrates two points. First of all, Design Thinking is a vivid practice and true to the *Design Thinking Mentality* as a way of thinking creatively and progressing non-linear. Secondly, depending on the background or field of application it is highly possible that Design Thinking is understood and practiced differently. Especially the motivational factors of why an organisation starts using Design Thinking can vary substantially. It is seen as a tool for innovation by some and as an inherent procedure by others. Likewise, some see it as a set of procedures and methods while others define it as a mindset. But most authors agree on Design Thinking being used to solve some sort of problem focusing on humans. It is definitely not a coincidence that Design Thinking is received differently in a i.e. software development field where there are other practices and mindsets in use already than in a traditional product design environment where design itself has a completely different annotation to it already. In any case, it suggests that Design Thinking is not a behemoth with one single universal truth to it, but rather a constantly evolving technique that bends itself to suit the needs of an according environment. For that reason, this thesis will aggregate the previously stated definitions and form it into one that will be used as a reference definition for the work:

'Design Thinking is a work mode that allows finding alternative solutions to human-centred needs and problems by using creative ways of thinking, personalised tools and iterative process methods.'

3.2. Design Thinking Principles

Now that we have a clear understanding of what Design Thinking actually means, it is time to take a look at its principles. Here too it is possible that different individuals, groups or cultures have a different understanding or focus on other parts of Design Thinking and therefore come up with varying principles. For that reason, this section will first be used to analyse principles and then evaluate them according to the grand scheme.
In [10], the authors present a number of principles, but they also highlight that they only treat the most important ones for the sake of brevity. The principles they mention are the following:

1. *Innovation is made by humans for humans:* The authors describe the importance of this principle

as if there was only one allowed, it would be this. The most important aspects of Design Thinking reduced to a few words. Human needs are what drives innovation.

2. *Combining of divergent and convergent thinking:* This principle refers to the unconventional thinking of solutions that can show the way to almost unimaginable heights, and the subsequent narrowing down of ideas to only a few options that are deemed to be ”feasible”.

3. *Fail often and early:* Since Design Thinking is a highly iterative endeavor with multiple ideas and solutions being presented only for them to be discarded again, it is seen as a positive factor to make mistakes and learn from them at an early phase. Trial and error with the customers is key in evaluating and developing an idea or a solution.

4. *Build prototypes that can be experienced:* User or customer experience is a highly important factor of Design Thinking. Therefore, having a ”playable” prototype is of immense value. People can test an idea and their reactions and interactions will show the true value of this idea. Testing an idea can come in various forms and use different technologies or means.

5. *Test early with customers:* Similar to the principle of ”fail often and early”, testing an idea with customers will show the viability of the idea and therefore whether or not more energy and efforts need to be put into it.

6. *Design never ends:* This principle builds upon the idea of iterative work on an idea that incorporates experiences and knowledge of previous iterations and shape an idea closer to what the user wants.

7. *Design Thinking needs a special place:* Successful Design Thinking requires a specialised working environment to support the workflow and to yield positive results.

These principles are again repeated in [13]. As pointed out by the authors, the fourth principle, ”building prototypes that can be experienced” is a direct contrast to how it is usually done with information systems that utilise abstract models in their design phase, which can be hard to understand and hard to follow.

The authors of [11, 15] take a slightly different approach. They conclude that the number of Design Thinking principles can be reduced to four fundamental principles:

1. *Humans as a basis:* Human needs are seen as the basis for all operations. These needs have to be understood to enable innovation. Market viability is however named as a factor in the decision process where a new idea or product is chosen, according to technical possibilities.

2. *Multidisciplinary teams:* Teams consisting of four to six people of various background must be formed. As for a male/female-ratio, 50% is stated as the ideal value to have a balanced environment. The same balance should be achieved with the disciplinary backgrounds of the participants.

3. *Iterative process:* Iterative processes are meant to offer an opportunity to re-work a product and to give every member of the team a chance to contribute their expertise.

4. *Creative surroundings:* The principle of creative surroundings states that it is essential for creative work and the generation of innovation and ideas that the surroundings support such endeavors.

Furthermore, in their work [11, 15, 16] the authors state desirable personal attributes of the people that join a Design Thinking team. They should be *optimistic, empathetic, adventurous, cooperative*, and be able to do *integrated thinking*.
Another important aspect of successful and innovative Design Thinking is the surrounding area and the work environment[11, 15, 9]. Some authors see this not only as a method, but also a principle. Creative and innovative work can be hindered by sterile and standardised office environments. There are three reasons identified by [9] why it is important to have a specialised Design Thinking location. First of all, because out of necessity to work ”in the field” and with users, be it during the empathise or testing phase. Secondly, creative work behaves differently and therefore requires a different set of tools to work with, similar to how a mechanic needs his workshop, creative work benefits from having its own dedicated *creative office space*, atelier or studio. These premises should also be equipped properly with i.e. drawing boards and craft stuff. The third aspect is the working atmosphere. Within the premises of creative work, it is highly encouraged to abolish hierarchical structures and instead promote the idea of fully cooperative work. A creative team needs to work as one unit without fears from one to another. This in turn also means that feedback and criticism must be appropriate.

3.3. Measuring Design Thinking Success

Investing in the implementation of Design Thinking can be costly, as pointed out in [12, 27]. From a business strategy perspective, it is not only recommended, but might even be necessary to take measurements and calculate a return of investment. Accounting for Design Thinking as a strategic resource within a company and thus granting it strategic value is what separates individual use cases from systematic long-term approaches.
In [12], the authors describe a number of relevant metrics for Design Thinking. The proposed metrics are not equally useful for all types of businesses, with some catering more to traditional companies that

only operate locally and others that are clearly meant for enterprises with a strong online-presence. The metrics are *Foot Traffic, Inquiries, Sales, Referrals, Impressions, Click-Throughs, Content Subscriptions, Page Views, Follows and Likes, Satisfaction Ratings*, and *Churn*. When it comes to measuring the performance of small enterprises or companies that are new to using metrics to measure performance they recommend selecting only a small number of relevant metrics, but measuring should happen on a regular basis. When it comes to measuring the effectiveness of a Design Thinking project it is suggested to take measurement snapshots before and after the project.

As pointed out by [27], measuring the success and impact of Design Thinking is not plain sailing. There are multiple other factors surrounding any company that contribute or hinder the success of a Design Thinking initiative. It is also highlighted that depending on the degree of strategic involvement of Design Thinking in a company, an entirely different set of additional metrics might be relevant for a company with the previously mentioned *customer related metrics* only taking up a small spot on the overall possibility of measuring the impact of Design Thinking.

4. Design Thinking Tools and Techniques

As mentioned by [10, 13], it is impossible to describe every tool in existence that could be used in Design Thinking. It is also stated that Design Thinking practitioners usually draw from more than a hundred different tools during their Design Thinking work, depending on which would be suited best to deal with a certain situation. This thesis is not aiming at becoming a glossary for Design Thinking tools and therefore won't cover such a quantity. Of course, important or often-used tools will be listed and explained in this work, but niche tools and applications are not the focus.
Additionally, it must be said that there are two different sets of Design Thinking tools. One category are the tools that are used as part of a Design Thinking Process to progress through the individual stages, tools that are used by Design Thinking practitioners on their quest to the final product. The other set of tools are supportive Design Thinking tools that are used to plan, coordinate or enable Design Thinking. To give an example: A *Customer Journey Map* is a tool used during a Design Thinking phase to get closer to a solution. The *Touchpoint Dashboard* [64] on the other hand is a tool used to craft such a map. Since this thesis does not aim at comparing such supportive tools, the ones that do get a mention will also be the ones that are used in a later phase of this work.

4.1. Supportive Tools

As previously mentioned, this section will provide an overview of Tools that enable the Design Thinking workflow and offer support for the individual tasks.

4.1.1. Miro

One of the tools used in this thesis is the collaborative online tool *Miro* [65]. Miro serves as an online whiteboard workspace where multiple people can work together in a creative was. It offers additional features like presentation modes and video chats, to support many digital workflows. It is especially useful for Design Thinking, as it allows for many creative work modes and offers a wide range of templates for various Design Thinking tools [66].

4.1.2. Mural

A direct competitor to Miro is the online tool *Mural* [67]. It is a ”digital workspace for visual collaboration” with an online whiteboard at its core. They offer a variety of templates for agile workflows as well. The templates it offers are of the categories Brainstorming & Ideation, Strategy & Planning, Meetings & Workshops, Client Engagements, and Design, Research & Analysis.

4.1.3. Mitre Innovation Toolkit

The *Mitre Innovation Toolkit* offers a wide range of templates for creative and Design Thinking work. These tools are sectioned into the phases scope, define, understand, generate, and evaluate. Each tool is explained in detail, even including the number of involved persons and a suggested time frame. Additionally, all templates are available for download to further facilitate Design Thinking work, as any person involved would therefore not be bound to a computer [68].

4.1.4. IBM Design Thinking Toolkit

The *IBM Design Thinking Toolkit* works in a similar way. It provides an overview of several Design Thinking activities, categorized by their ”area of the loop” and the stage of the Design Thinking process. IBM chooses a two-tiered approach that will expand its offerings based on a registered account, opposed to free access of the entire toolkit [69].

4.1.5. IDEO Design Kit

IDEO is a non-profit organization focusing on Design. Their *Design Kit* is sectioned into the areas inspiration, ideation, and implementation. They offer a large variety of different tools, with each of these being described in detail with a step-by-step guide. Additionally, they offer a series of questions to help inexperienced individuals to find a fitting tool for their purpose [70].

4.2. Stakeholder/Community Map

A stakeholder map is used to identify any person or group of people that might by affected by the project in any way or form. It is advantageous to create this map with a broad and liberal understanding of the term stakeholder, as it is better to include more and extreme edge cases than to omit a group that turns out to be immensely important in the end. Especially end users are an important stakeholder [10, 13]. For the creation of the map, a full list of all stakeholders is required for a holistic view. Compiling such a list may take a lot of effort and aims at even revealing stakeholders that were not thought of previously, as

well as highlighting important connections between them. It is an effective tool for any decision making process on where resources should be focused or invested in for the best outcome [21].

4.3. Service Safari

A service safari is a technique especially used in *Service Design Thinking*. It aims at evaluating a service experience and finding good examples of services. It is advisable to have a template to follow for the service evaluation so that the results can be compared more easily. The targeted services are usually similar to the one that is to be implemented, but it is equally as valid to evaluate any service in the quest for a good service experience from the point of view of a customer [21].

4.4. Empathy Map

An empathy map focuses mainly on end customer analysis, but can be applied to any stakeholder. The tool focuses on what the people tell i.e. during an interview. Their acts and statements get split into four sections: *Say, Do, Think*, and *Feel* [10, 13, 23]. Personas are often used as a input for empathy maps to better understand users [11]. A better understanding of the users and their environment will create empathy for the targeted representative individual and thus elevate our understanding of their needs and provide further insights [17, 23].

4.5. 5-Whys

This method is not exclusive to Design Thinking and will be familiar to those working on root-cause-analyses. Unlike the name suggests, there is no strict rule to ask ”why” exactly five times. It is a mere reminder to keep repeating the question until the root cause is identified [10, 13]. However, other authors [21] claim that it could negatively affect the results when going into more depth than the fifth ”why”, because the focus on the initial problem could be lost. It is however a very useful technique to scratch the surface and identify problems.

4.6. Interview

Similar to the *5-Whys* method is the user interview, with the difference that questions are not asked to find a root cause for something, but rather to reveal motivations, thoughts and emotions of a user that arise during the use of a prototype, service or product [11]. It is advised that an interview guideline is used and that the questions are tailored according to the context. Question could be about general

matters, specific details or about comprehension. Another form is the specialist interview, which is used to gather expertise and insights on a certain topic. These ideally empathetic questions should help the interviewed person to open up and overcome barriers, as it usually takes a long time during an interview until a person feels confident enough to be completely honest [14, 21].

4.7. AEIOU

AEIOU is not related to the motto of the Habsburgs, as the name might suggest, but rather an acronym of the dimensions used to organise data [10, 13]. The dimensions are *Activities, Environment, Interactions, Objects* and *Users*. By splitting a problem into its dimensions, it can reveal important connections between said dimensions.

4.8. Persona

A Persona is a tool used to create the fictional existence of a human being that is used to represent a larger portion of the target audience. Personas are used as a reference point during the Design Thinking processes that the practitioners can work with as a more accurate and in-depth visual of a broad mass of people [10, 13, 19, 21]. Personas can i.e. be created from previous results of interviews, observations or the results of a stakeholder mapping and they should be distinctly different from one another to cover as many perspectives and needs as possible [11, 21]. Each persona has a set of characteristics that are used to describe a representative person for a whole group of users. These characteristics usually include demographics, as well as goals, needs and other information about them [17, 19].

4.9. Observation

An observation is used to see someone, i.e. a user, in an undisturbed and real environment which makes it possible to observe how a person reacts or uses something compared to how it is intended to be used. This undistorted view yields valuable information about a product and whether there is need to refactor [10, 13]. As further elaborated in [11], the observer must write down notes and create an observation protocol, which in turn can be analysed in more detail later on. Such a protocol can include the activities of the user, how something is done and why it is done. A major benefit of observing or *shadowing* is that an observer can experience the immediate and natural reaction of a user whenever a problem occurs [21].

4.10. Storytelling

Storytelling is used to properly present an idea [10, 13, 23, 25]. Not only is it supposed to be more effective when it comes to attention, but it is also a useful tool to portrait an idea in a real world situation, especially when used in combination with other techniques that are suitable to illustrate such an idea. When the right narrative techniques are used to present a story it can have a major impact on the listeners. Furthermore, ideas that might sounds like a good option within their idea generating environment could turn out as subpar when told in a story. [21].

4.11. Story Boards

Story boards use pre-defined personas as a basis and present the process of using a product or service in the form of something similar to a film script or a comic script that includes various scenes with information about what is happening when and by whom, and in the case of Design Thinking especially, what they feel while doing it. Supportive text and images are used to further elaborate on any given scene [19, 21].

4.12. Journey Maps

Journey Mapping is usually used in the context of either customers or users. Both of these have a different purpose and therefore yield different results [71]. While a *customer journey mapping* focuses on the customer experience as a whole, including both digital and physical touch points throughout the entire customer process, a *user journey mapping* deals with user experience and is usually found in the context of UX testing of applications or websites. A journey mapping is used to evaluate a service, product or process from the point of view of a user and to reveal further needs or problems of a user in the process [11, 23]. Others describe such maps as a tool to document and lay out the journey of a user from beginning to use something up to the level of being proficient [24]. A Journey mapping can be useful to structure and condense previously gathered information about users to one streamlined visually represented process which is easier to work with [14]. Especially in the field of service design, the customer journey map is a highly important tool, as they are often used to visually represent the entire customer experience and the path of a customer before, during and after a service is used [19, 21].

4.13. Service Blueprints

A Service Blueprint is, as the name suggests, used in *Service Design Thinking*. They serve as a model canvas for a service where details and nuances of the whole package can be planned and visually represented. It is important to include the views of important stakeholders into the creation of a new service, which should be part of any Service Blueprint. Routinely revising the document and making sure that its contents are still correct and incorporating all necessary aspects of its environment are needed to keep the blueprint alive. Specified touch points between the stakeholders make it apparent where co-operation might be needed and what redundancies there are. A good blueprint can act similar to a process mapping [21].

4.14. Idea Generation - Brainstorming

Brainstorming and Brainwriting are used when it comes to the Design Thinking phase *Idea Generation* [11, 23, 25]. Previous problems and needs of users or defined personas are used as a basis for this act. The difference between Brainstorming and Brainwriting is that in Brainwriting an idea can also be noted as a visual representation of sketch. The generated ideas have to solve a problem or cater to a need. It is advantageous to have a set template for the notation of ideas that includes what it is trying to solve, what and how it should be done and whether there are already existing approaches on the matter. In the end, all ideas are clustered and deduplicated. These resulting ideas can then be used in the next Design Thinking phase. It can be beneficial to re-iterate ideas to come to a more specified and specialised conclusion [14]. It is important however to remove any form of criticism or judgement of ideas at first and evaluate ideas at a later point to not hamper the generation of new ideas [17]. Other techniques that are used to generate ideas are *Mind Maps,* the *Six Thinking Hats* method or a *SWOT-Analysis* [21]. Each technique works slightly better or worse with certain topics, that is why a Design Thinker will ideally choose the most optimal form of idea generation to synergise with the problems or goals at hand.

4.15. Prototyping

Prototyping consists of the three stages of *prototype development, prototype testing* and *prototype integration*. During the first stage, prototype development, the previously generated ideas will be turned into a prototype [11, 25]. Prototypes can come in various forms. They can be sketches of the product or service where illustrations explain everything. Other methods call for stories that describe how a user acts with the product. These should usually be tied to user journey so that the intended user experience can be put

into the picture properly. It is also possible to create films, animations or mock-ups of the product that show how it is done. And of course, the most traditional option, the creation of a physical model made of cardboard or other craft stuff. It is also possible to create prototypes with a multitude of different forms. It is advisable to start with a minimum viable prototype so that changing it later on does not result in a great loss, as it is highly likely that there will be multiple iterations of any prototype [14, 21]. There are different forms of prototyping where each aims at completing a different objective [23]. Prototype testing can be done to ”test” empathy to point out what is on people’s minds, it can be a functional test of course, or a test as a basis for further decisions.

Once a prototype reaches a certain level of maturity, it can be tested by users. During such a test it is important to observe the behaviour of the users for the duration of the test, to ask them according questions and especially to document the test. Part of the documentation is also the user feedback. All these factors contribute to the evaluation of a prototype. Depending on the results, a prototype can either be scrapped, reworked and tested in another iteration, or be integrated into a running system [11, 23]. Iterative reworks and testing of prototypes is an important tool, especially for usability testing. In its very core, the iterative methodology is also used in agile development environments [19, 21].

When all previous testing is successful, a prototype can then be turned into a business model and consequently be integrated in the overall existing business processes to start generating value for both the company and its customers or users. One benefit of such an integration is to gain a competitive advantage on the market [11]. There is a multitude of dimensions that determine the business model, i.e. financial dimensions or customer dimensions.

5. Design Thinking Processes and Models

Since the idea of Design Thinking first emerged, there were multiple approaches on trying to arrange it into a more structured and streamlined procedure. A clearly defined process is helpful when it comes to teaching and expressing the individual work stages of Design Thinking. However, it is emphasised that models and processes are merely supportive tools and not meant to be followed strictly, as creativity should not be hampered by strict rules [9, 63, 23].

5.1. Five-Phases-Model

One of such processes is a widely accepted *Five-Phases-Model* mentioned, amongst others, in [9, 63, 23]. This process is sectioned into the following focus areas:

- *Empathise:* This part focuses on how a certain individual or group of humans perceive a situation or a problem. What they need, feel or suffer from is to be apprehended and viewed subjectively.
- *Define:* During the *Empathise* step, important insights and views are generated generated. These can be bundled together to create personas which are then used to specify exact problems and needs of users.
- *Ideate:* This step is similar to a brainstorming. It is the objective to generate as much ideas for viable solutions as possible, so to have a wide range of options to work with.
- *Prototype:* From all previously emerging ideas a few are selected and turned into prototypes. With these prototypes the idea is then tested. The most important aspect for deciding whether an idea is good or bad should be what the users experience and feel during these tests.
- *Test Solutions:* After successful prototyping, it is now time to propagate and test the solution in a real world environment.

A visual representation of this process can be seen in figure 5.1. While pointing out that there should not and cannot be one single structure to dictate how Design Thinking works as it is always bound to change

depending on the situation at hand, [12] and [20] offer a slightly different model consisting of the five phases *Understand/Empathise, Define, Ideate, Prototype* and *Test*. At first glance, it appears to be very similar to the model presented by [10], especially the last three phases, but there are differences. The model can be seen in 5.2. In the first phase, a pre-existing challenge needs to be understood. According to this model, the challenge/problem does not have to be defined by the Design Thinkers themselves, but is rather taken as something that exists. After learning about the challenge, it has to be unmistakably defined and also why it is a problem in the first place. Ideate is again used for brainstorming and finding new ideas and concepts. The best ideas will then be turned into fitting prototypes and tested accordingly. With tests, an idea can be evaluated on a smaller scale. The authors point out that since all Design Thinking work is creative and non-linear, it is possible to swap or repeat certain phases.

Figure 5.1.: Process model of a generic Design Thinking process [9, 63].

Figure 5.2.: 5-Phases Design Thinking Process Model according to [12].

5.2. Design Thinking Micro Process

Another representation of a Design Thinking process is the ”design-thinking-micro process” from Stanford University [10, 13], as shown in 5.3. This process shows the very nature of the iterative mindset for incremental improvements towards near perfection. This cycle is highly focused on the experience of and work with users/customers to refine the solution or product. Working together with the users is not only encouraged, it is needed to guarantee success.

- *Define the problem:* The problem is defined in the form of a question. These questions should be formulated in a way so that everything relevant is within the scope.

- *Needfinding & Synthesis:* This step highlights the needs of a user, both overt and covert. It is also used to get the needed knowledge for the project.
- *Ideate:* Brainstorming based on the defined problem and needs.
- *Prototype:* Creation of prototypes of a fitting ”resolution”.
- *Test:* Testing of the prototypes with the users/customers for the users to experience an idea.

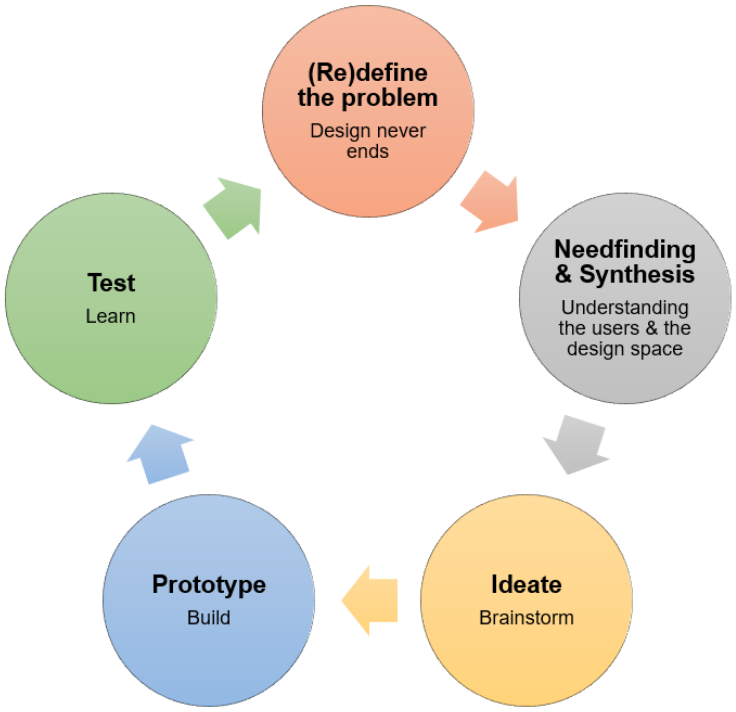


Figure 5.3.: Stanford University Design Thinking Micro Process [10].

5.3. Seven-Stage-Process

In [11], the authors describe a seven-stage process for Design Thinking work. Their process starts with the definition of a challenge and ends with the integration of a new prototype of an idea or product into an existing modus operandi. This process model can be seen in 5.4. The strength of this process is that can be used for the integration of new content into existing systems, whereas the previous models have more of a generic approach that focuses on the product itself and has less regards for its business surroundings.

Figure 5.4.: 7-Phases Design Thinking Process Model [11].

5.4. Double Diamond

The process described in [14] is called ”Double Diamond” approach, shown in 5.5. It is characterised by the two stages called the ”Problem Space” and the ”Solution Space”. Each of these is further divided into a divergence and a convergence phase. During the first phase, *Discover*, research data has to be gathered. Qualitative data should be the one to go with. It is important to get the information about how and why a user or customer decides to do something and what emotions and feeling are triggered in the process. The more information that is gathered in this phase, the better. The second phase, *Define*, is then used to structure the previously gathered information and to generate insights. The most relevant information can be extracted and connections between points of interest are made. Especially the cause-effect-interaction is important in the analysis of human action and behaviour. Various tools can be used to properly map the information to a specifically defined solid insights. With these definitions, the ”Problem Space” is finished and the *Develop* phase begins. In the second divergence phase, the Design Thinkers have to generate ideas and solutions to the previously set definitions. This phase profits from creativity of the people involved. All the ideas that are now at hand have to be evaluated and reality-checked. A selection of ideas will be turned into prototypes, which will be tested in the *Deliver* phase. The important note is that in this phase the subject of delivery are the results of the ”Double Diamond”. If the results are not satisfactory, a new iteration of the entire process should follow.

Similar to Double Diamond is the *Divergent-Convergent Inquiry based Design Thinking Model* (DCIDT), presented in [16]. In this model there is only one ”diamond”. Within this diamond there are still diverging and converging phases supported by according questions, inquiries, and reasoning. This model is focused on generating and evaluating design concepts. There is however no phase included that would allow for user interaction, prototyping or testing.

Another model proposed consisting of continuous four phases [16] is arranged in a similar way as other continuous improvement cycles. This process model for Design Thinking is split in the four phases of *Abduction, Deduction, Test*, and *Induction*. The first phase focuses on the generation of new ideas. These ideas will then be evaluated in the next phase. This evaluation takes into account possible consequences of an idea. After this evaluation step, the testing phase begins. Where an idea yields positive results, it is then generalised in the induction phase. What sticks out about this model is that it is meant to be

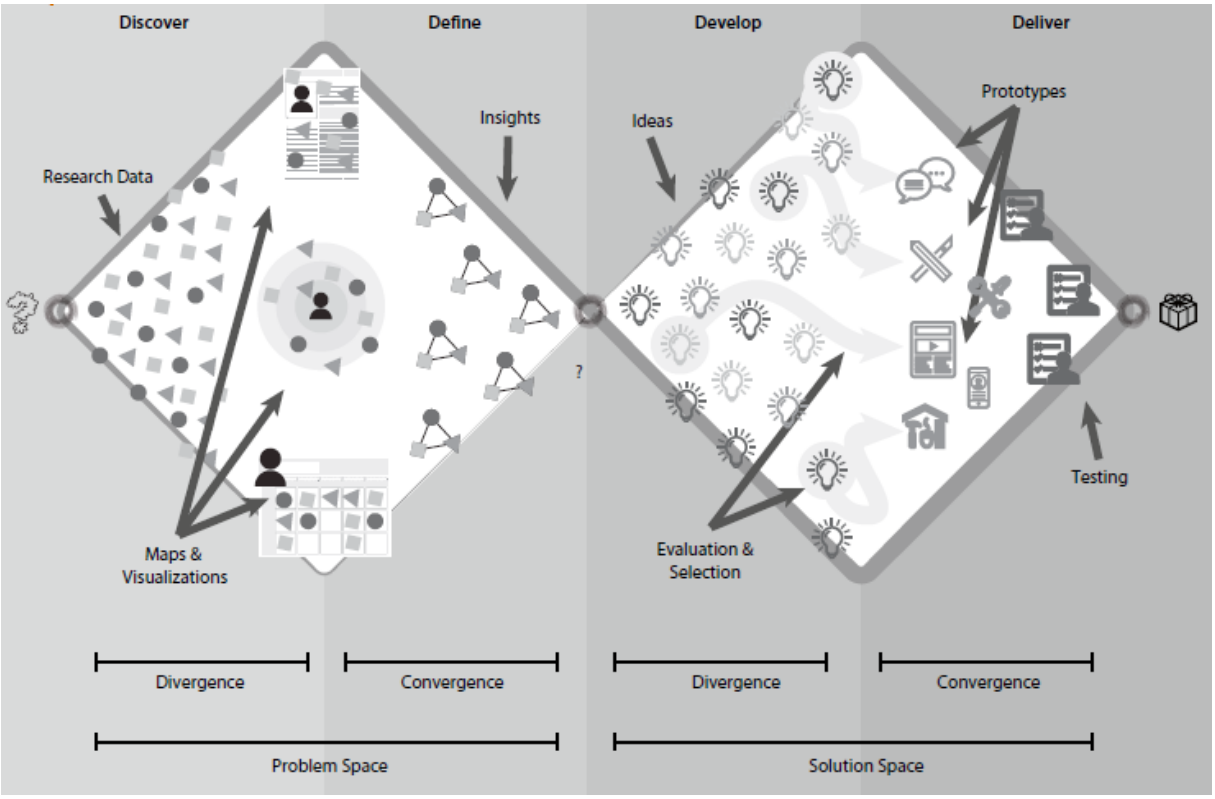


Figure 5.5.: ”Double Diamond” approach of Design Thinking [14].

a continuous cycle but there is no specific phase for detecting problems or needs of users on which the generation of new ideas could be based.

5.5. Design Thinking Spaces

A different approach is explained in [16], which is also mentioned in [17, 19], and it consists of *Inspiration, Ideation*, and *Implementation* in the form of ”Design Thinking Spaces”. These three are the process model spaces which house a number of activities. An activity from one space can overlap and be part of another space as well. Furthermore, there is no strict rule about when or where an activity must be done. This is done to support the creative flow. There are however general directions for each space. The inspiration phase is generally used to establish a working foundation by specifying problems, needs, and opportunities of a human-centred observation. This foundation is then used in the ideation space to generate, test and evaluate emerging ideas. When an idea is successful it can then be implemented in the implementation space. A visual representation of the three spaces can be seen in 5.6.

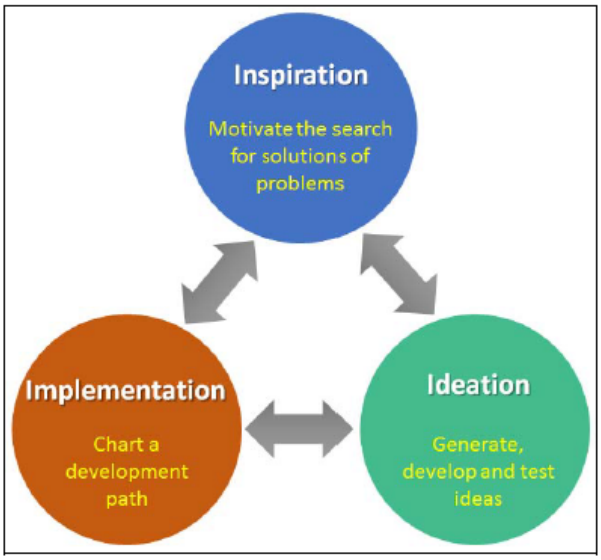


Figure 5.6.: Design Thinking Spaces [17].

5.6. Design Sprints

Design Sprints are explained as a method that combines Design Thinking with Agile practices for faster prototyping and testing [24, 72]. They are specifically meant to take on and overcome design problems within one week. Design Sprints were originally created by Google Ventures and are heavily used there. There are technically no limitations on team sizes for a Design Sprint, it is however essential that there is a *Sprint Master* taking the lead. This person is usually the one that identified the design problem that needs to be overcome with the sprint and similarly is responsible for guiding the team through the stages of the Design Sprint. The ideal personal profile for such a role is that of a UX researcher or designer. A sprint itself consists not only of the sprint phase alone, there are certain tasks that need to be done before and after the sprint and it is advised that the preparation phase should be the same amount of days as the sprint phase. The individual phases of a Design Sprint focus on the following:

- Sprint Preparation: The most important part of the preparation phase is that the problem or design challenge is adequately selected and specified. As part of this primer it is important to also define deliverables and for whom a solution to the problem is beneficial. Other than that it is important that a Sprint Master needs to communicate the challenge and carefully plan and prepares all needed resources, including the team members.

- Sprint: During the sprint the Sprint Master has to pull the team through with a clear focus in mind, but at the same time with regard for the planned schedule and prepared exercises. Generally speaking, a Sprint Master can be seen as a guide for the team at this point.

- Sprint Retrospective: When a sprint comes to an end, there should be some form of follow-up both creatively and in the form of a continuous improvement survey. It is also the time to talk about eventual further sprints.

5.7. Discussion - Design Thinking Processes and Models

Although several different models and processes of Design Thinking were introduced in this chapter, most of them share the same principle ideas in both structure and expected results. There are a number of elements that have the exact same purpose across the different Design Thinking process models. Usually there's a point where a problem or challenge gets defined to set a foundation from which the process continues. There's also always a phase where ideas are generated. Whether it is called brainstorming, gathering ideas or ideation, the result is the same. By divergent thinking a number of possible solutions to address and ideally solve the previously defined problem have to be generated or created at this point. From that step onward, the models focus on the most promising of them and start to design, create and test prototypes. Some of the models differentiate between the individuals steps, others see it as one overarching phase of prototyping. Differentiating between the individual steps of the prototyping phase could be beneficial however, if the team of Design Thinkers and Prototypers has enough resources and a structured working environment to allow for these clear boundaries. On the other hand, differentiating the steps could hamper the creative process as there it could lead to a confined environment where switching back to a previous step is not possible, as it would break the process cycle. It is therefore advisable for each Team of Design Thinkers to think about their working environment and problems that need to be solved, so choosing the most appropriate working mode is possible. The last phase of the different processes that is similar between them is that they all have a phase for validating the work. Whether it is validation or testing of an implemented prototype in a real world scenario or simply a validation of confirmation to customer needs. In the end all models focus on delivery and especially the quality or viability of the Design Thinking results.
To summarize, a Design Thinking model or process can be reduced to and described by asking three crucial questions:

- What do I want?
- How do I get there?
- Did I achieve my goals?

To further elaborate on this, the first question expresses that in the begin of each Design Thinking process it is important to get a clear understanding of the problem, its environment and what the most important

factors are. This can be done by a number of different techniques that focus on information gathering, analysis and assessment amongst others.
"How do I get there?" symbolizes the phases of generating various ideas to the identified problems and to come up with actual solutions that can be delivered as a product, service or agreed on deliverable after finishing one complete modeled process.
Once the deliver phase is over it is crucial to actually evaluate and assess what has been delivered retrospectively. This could be done to either assure quality levels and standards of a delivered product or simply to know if the delivered product is actually solving the problem that has been specified beforehand. If a product fails to satisfy the needs of a customer, the cycle must repeat.

The only notable difference is presented by *Design Sprints*. A Design Sprint is less of a Design Thinking process or model itself and more of a Design Thinking framework. As previously mentioned, it combines *Agile Working* with the domain of Design Thinking and offers many new opportunities in the form of a structured high level concept that still allows and accounts for flexibility and creative work, but at the same time it ensures that momentum is maintained. So a universally valid Design Thinking process model can be part of one Design Sprint. Additionally, the concept of Design Sprints highlights the idea of continuity of Design Thinking by suggesting that one sprint comes after the other and that there is a continuous improvement or continuous problem solving at hand.

6. Information Security

When it comes to information security, a lot of effort goes into explaining the importance of implementing a proper system. In the light of ever increasing numbers and varieties of cyber crime [3, 1, 6, 73, 74], protecting information adequately should become a priority for both private individuals and companies alike.

Information security itself may be a fuzzy term for those unfamiliar with it. To shed light on the matter, the term itself can be split up in several important components. This is visualized in figure 6.1. The foundation of it all are *confidentiality, integrity,* and *availability*. These are universally seen as the core element of information security and will be explained in more detail in section 6.1. Network, data and computer security are also a rather obvious inclusion to information security, as ICT-systems are usually what is associated with information or cyber security. [75, 76, 37, 77, 78].

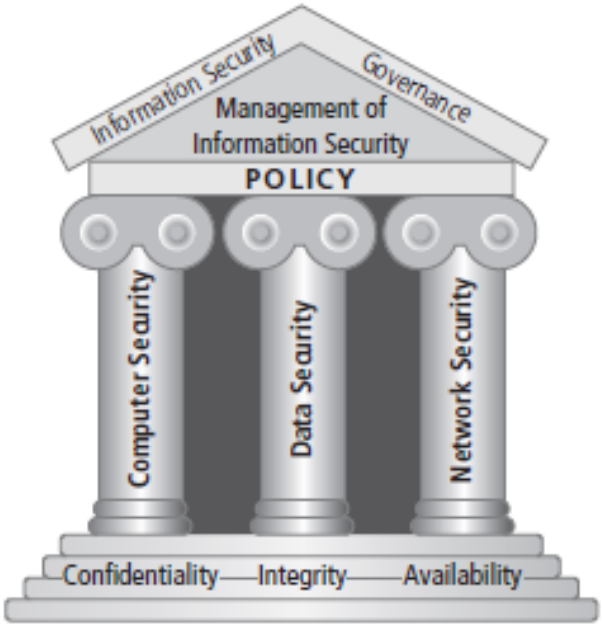


Figure 6.1.: The components of information security [78].

One way to ensure secure practices for the handling of information is the implementation of an *Information Security Management System*, (in short ISMS) [41, 73], which plays a major role in the world of

information security, as it is possible for organizations to certify their security levels with the ISO 27001 standard. Such a systematic approach reduces risks and mitigates threats, if well maintained and incorporated in the overall processes of an organization. The collection of all information security efforts within such a system is usually manifested in an *information security policy*. More on that in section 6.2 This chapter is used to highlight the fundamentals of information security and to provide a concise explanation of its principles, elements and objectives. Such an explication is important for interested parties coming from a field outside of information security or technology. Especially in the context of this thesis, where there is a strong focus on Design Thinking, a concise overview of what information security is and which elements matter functions as an important asset in the phase of cooperation between the fields so that all the people involved have access to a common set of definitions and therefore a shared understanding of the subject.

6.1. Information Security Principles and Pillars

At its very core, the fundamental basis and principles of information security can be found in the CIA triad. CIA stands for *confidentiality, integrity* and *availability*, and is usually termed as either the principles, objectives or tenets of information security. Each company will focus on these with a varying intensity between them, because depending on the organizational context and mission, the significance of one could be several times higher than the other or vice versa. These three principles can be explained as follows and are visualized in figure 6.2 [75, 76, 37, 77, 78, 38, 39]:

- **Confidentiality:** In short, confidentiality means that only an authorised person can access information. Security measures like access restrictions and to some extent even data privacy fall under this category. Theft or disclosure of information has to be prevented.
- **Integrity:** Integrity of data and systems means that they can be trusted and that there has not been any unauthorized manipulation, modification, tampering or (partial) destruction of information or information systems which guarantees the authenticity and trustworthiness of information. Non-repudiation and traceability are elements of Integrity.
- **Availability:** Availability is the third tenet of information security and it demands that access to information is unimpeded and reliable, as long as the request was made with the required authority. Availability of i.e. a web service could be infringed by a Denial of Service attack.

Of course, these three principles are just the foundation of information security and there are many more

Figure 6.2.: Confidentiality, Integrity, Availability - The classical Cybersecurity Triad [77].

that could be highlighted or part of a business strategy. Especially newer laws and regulations like the GDPR elevated the importance of a number of other principles, which focus especially on the processing of personal data [75, 47]. More on that in chapter 7.

It must be mentioned though that there is a second Triad revolving around information security [79]. While the classical triad of confidentiality, integrity, and availability mostly focuses on *how* information security is to be implemented and operated, the second triad with people, technology, and processes highlights *where* it will happen and *what* domains are affected. ”Technology” is the most obvious part of these three, as it usually are ICT-systems that come to mind when considering information or cyber security. The domain ”people” might come as a surprise at first, but as already mentioned in chapter 1, the human factor is without a doubt responsible for a major part of all information security issues as it is often times the weakest link in the defenses. Securing the human factor is an important undertaking for organizations of all sizes and regardless of whether they have an ISMS implemented or not. Processes and policies on the other hand show that there is a higher maturity, as these are usually elements of an organized information security effort with a systematic approach that also considers roles and responsibilities. This becomes apparent with the fact that certified information security includes these elements [41, 80, 79, 38]. This triad can be seen in figure 6.3.

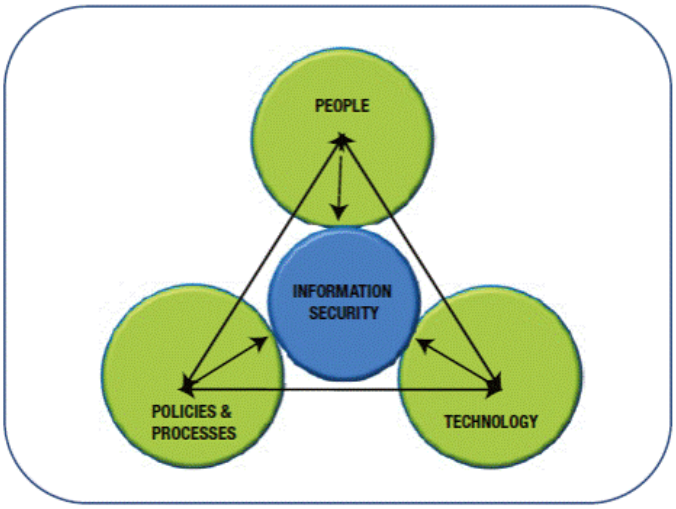


Figure 6.3.: Pillars of Security - People, Processes, Technology [79].

6.2. Information Security Policy and Security Leadership

6.2.1. Information Security Policy

As previously mentioned, an information security policy is an essential part of an ISMS. In [78] it is defined as ”a set of rules that protects an organization’s information assets” and it serves as overarching ”law” where correct and incorrect behavior is written down. High-level concepts of how information security will be handled are included in such a policy document. Such a policy should fit the organizational context and mission, and enjoy the support and commitment of the top management to be effective. This document should be made available and thus not contain sensitive information. Generally speaking, a policy is a set of rules, expected behavior and managerial statements. An information security policy specifically describes what is necessary to reach set security objectives and how these will be protected long-term. A company is not restricted to one single policy however. It is absolutely viable to go into more detail in subject-specific policies i.e. a *Bring your own Device Policy*. This becomes clearer when separating policies into company-wide internal standards, guidelines and procedures with each of them being more detailed and technical than the previous one. Procedures can be seen as a manual for a certain task that should be followed by everyone doing said task. A guideline offers more freedom during the implementation of a security measure or while completing tasks. They are simply meant for guiding a person so all obligations are met in the end. Internal standards function as the ”company law” which should be followed by all employees. These standards focus on company-wide implementations or behavior that is critical to all, i.e. mandatory participation in awareness programs [41, 73, 37, 81, 75].

6.2.2. Mission and Management Commitment

As previously mentioned, the success and effectiveness of information security endeavours is critically linked to the organizational context, its mission and the degree of integration of information security processes into business processes. It is important to understand the needs and requirements of affected parties, as well as to understand the importance of underlying ICT systems to achieve the mission. Additionally, once the mission and organizational strategy are clear, the definition of information security objectives linked to this cause are the next step. Likewise, leadership and management commitment are critical success factors for any information security endeavor and especially for an information security management system. Information security decision making is usually based on risk assessments, which is even a requirement for an ISMS, to determine the degree of necessary security measures. Once there is an existing information security strategy or procedure, all affected parties should be informed about it accordingly [37, 41, 81].

6.2.3. Information Security Roles

Accountability and auditability are important factors in the field of information security. Defining a series of roles with respective sets of responsibilities helps to form a personal connection to security issues and needs, as well as it is an important part of installing authorities and dividing responsibilities. Such roles can be used to delegate certain tasks to the most relevant person, and to simplify communication channels. Security or system owners should be written down in the information security policy [41, 73, 37]. Important roles in information security are the following:

- **CEO**: As the highest-level executive the CEO is responsible for merging information security management with the rest of the company. This includes the implementation of required security measures and compliance to legislation.
- **CIO/CISO**: The *Chief Information Officer* or *Chief Information Security Officer* is responsible for task like the allocation of needed resources, security program implementations and system protection.
- **Information Owner**: An information owner must define the security requirements of the respective information and how it should be protected.
- **System Owner**: In the context of information security, a system owner is responsible for the implementation and maintenance of security measures, as well as ensuring compliance of the system to security requirements.

- **System Administrator**: System administrators are responsible for the underlying ICT infrastructure. This includes installing, configuring, updating and maintaining of the systems, performing recovery and backup tasks, as well as the implementation of technical security measures.
- **User**: A user must follow internal policies about the usage of ICT systems and report unexpected behavior.

6.2.4. Information Security Governance

The online edition of the Cambridge Dictionary defines governance as ”the way that organizations or countries are managed at the highest level, and the systems for doing this” [82]. Coupled with information security this then means managing and steering information security at the highest level with all that is included or required. Main elements of information security governance are the establishment of strategic goals and directions that an organization wants to take and an according measuring and progress assessment of the same. This includes the verification and validation of risk management and asset use [78].

6.3. Information Security Management System - ISMS

As already mentioned before, the ISO27000 series and especially the ISO 27001 is an extremely important framework in the field of information security [78, 73, 41, 83]. It is a systematic and controlled framework to introduce, operate, and continuously improve an information security management system. This means that any organization with a certified ISMS is more likely to be trusted with issues of that sort than an organization with no proof of the security levels of their ICT-systems. The overall structure of the ISO 27001 is similar to that of other management systems (i.e. that of the ISO 9001 [84]) and contains the following chapters [41]:

- Context of the Organization
- Leadership
- Planning
- Support
- Operation
- Performance evaluation

- Improvement

The system described in ISO 27001 is supported with guidelines in the form of a ”Code of practice” in ISO 27002 [80, 78]. It includes the following chapters:

- Information Security Policies
- Organization of Information Security
- Human Resource Security
- Asset Management
- Access Control
- Cryptography
- Physical and Environmental Security
- Operations Security
- Communication Security
- System Acquisition, Development, and Maintenance
- Supplier Relationships
- Information Security Incident Management
- Information Security Aspects of Business Continuity Management
- Compliance

6.3.1. Monitoring and Continuous Improvement

A universal requirement for any ISMS or information security programs is a form of regular monitoring, performance evaluation, reviews or a *Continuous Improvement Processes* (CIP) [41, 73, 37]. These are a measure to ensure the correctness and functionality of a system or information security program and is useful for uncovering new threats to the security objectives of the company and risk assessments. Another part of continuous improvement is ensuring a well maintained information security system and awareness program. If awareness is insufficient, the entire information security system is questionable. One of the most well-known and widespread applications of a continuous improvement model is the PDCA model as a way of managing and improving processes involved with information security according to

the ISO 27001 [85]. This model (figure 6.4) is used to showcase how an ISMS should be implemented and managed and that a successful use of the model will turn mere requirements and expectations into a fully managed system.

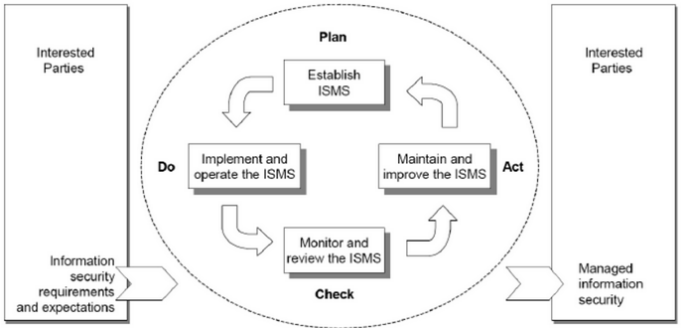


Figure 6.4.: PDCA model applied to ISMS processes [85].

6.3.2. Risk-based Approach

A risk-based approach is practically part of any serious management system. Especially in the case of information security it is the ISO 27001 that calls for such an approach to identify and adequately counter and control risks, so that the level of information security of an organization is not compromised [41]. This means that both the detection, assessment and management of risks, and the use of mitigation techniques and security controls are equally important for any systematic information security approach.

Risks and Information Security Threats A risk as defined by [78] is ”the probability of an unwanted occurrence, such as an adverse event or loss”. It is therefore in the best interest of any organization to minimize risks wherever needed. One term that is usually mentioned when it comes to risks and risk management is *risk appetite* [86, 78]. What it describes is the level of risks that an organization is willing to accept. Important elements of risk management are the identification and assessment of risks. Information Security is sometimes compared to warfare, as the one securing an organization one can become the defender of a castle. Risk identification and assessment is similar to inspecting the curtain walls of a castle and looking for weak or damaged sections. Knowing about these weak links will greatly improve the chances of success for a defender, as they can either be removed in anticipation of an attack or acted upon accordingly [78]. ISO 31010 focuses on risk assessment techniques and is therefore a perfect knowledge base for a structures approach on identifying and assessing the most accurate representation of existing risks within an organization [87, 88]. Especially its annex is of immense value, as it

contains a substantial list of different techniques which are all explained in detail. With this catalogue it is easily possible to pick the most fitting technique for a specific problem.

Risk Mitigation and Security Controls Having appropriate safeguards in place is a crucial part of mitigating risks, and securing and controlling an organizational environment. Moreover, controls and security countermeasures are needed to properly react to any form of threat or attack [78]. In the annex of ISO 27001 [41] the required security controls for an ISMS are listed, with further and a more detailed explanation to each of them being presented in ISO 27002 [80]. As pointed out by [89], there are many different types and categories of security controls. It is important to understand the focus point and capabilities of these categories so they can be properly implemented. The main distinction being made is between *physical, technical* and *administrative/organizational* controls. In addition to that, a control can either be of the types *preventative, detective, deterrent*, or *recovery*. Picking the right combination of controls is key for a well-functioning organization. Another approach to information security risk mitigation through the introduction of a security control framework are the *CIS Controls*, which are currently available in their eighth iteration [90]. This set of controls is split into three different so-called *CIS Controls Implementation Groups*, which are designed for three different types of organizations, where each consecutive implementation group contains all controls from the previous group and expands on it. These groups are 1) ”basic cyber hygiene” for smaller organizations with limitations in the field of IT, 2) for organizations that have designated roles for the safeguarding of the systems and 3) for organizations with designated security specialists. These implementation groups can help an organization choosing the right set of controls with their resources.

The implementation of controls and mitigations however proves to be a greater obstacle for smaller organizations, than it is for larger ones [91]. The reason for that is because small organizations are not able to commit the same resources to security and compliance as a large company is able to. Additionally, there is often a lack of needed skills and knowledge about security issues, which could in turn lead to ineffective controls where they are implemented. For such organizations it becomes even more important to follow a risk-based approach, as the limited resources should be spent where they are most needed.

7. Data Protection in Austria

With the General Data Protection Regulation [47], a series of clauses about the protection of the processing of personal data of natural persons were presented to the public. It is meant to protect not only personal data, but also digital rights. Its applicability includes all forms of automated or systematic processing of personal data within the European Union and affiliated regions. The legal framework of the GDPR is further refined on a national level in the Austrian Data Protection Law [92], which unmistakably presents data protection as a basic right of every person.
This Chapter provides a concise overview of the most important legal determinations on data protection according to the General Data Protection Regulation and the Austrian Data Protection Law for organizations in Austria. This information serves as a basis of knowledge for organisations interested in a compliant implementation of their data protection measures, as well as a general overview for any interested reader. The main orientation lies on the GDPR, as it is universally valid in the entirety of the EU. Where there are further specifications in the national law of Austria that is not already mentioned in the GDPR, these specifications will be included.

7.1. Data Protection Principles

Like with information security, there are several principles in the field of data protection. Especially with the coming into force of the GDPR, the General Data Protection Regulation of the European Union, these principles are no longer just an idea or rough guideline, but a legal requirement. As stated in the regulation, the principles are as follows [75, 47, 93]:

- **Lawful, fair and transparent processing concerning the data subject**: This principle shall ensure that no processing of personal data is without a legal permission or consent from the data subject, who must be transparently informed about the processing.
- **Limitation of processing purposes**: Processing of personal data is only allowed for a specific purpose, namely the purpose that a data subject consented to. Processing outside of the agreed on

purpose is unlawful.

- **Minimization of data collection**: The collection of personal data should be reduced to a minimum of needed data for the specified purpose of the processing of said data. Collection of data that is not necessary for the purpose of the data processing should be spared.
- **Accurate and up-to-date information**: Collected personal data must be accurate. This includes an erasure of personal data once the purpose that serves as a basis for the processing is no longer valid.
- **Storage limitation**: Once personal data is no longer needed for the specified purpose, it should be erased. It is however possible to store data for a longer period of time if it is done in the name of one of the following purposes:
  - Public interest
  - Scientific or historical research
  - Statistics
  - Protection of the rights and freedoms in accordance to technical and organizational measures
- **Integrity and confidentiality**: Similar to the principles of information security in chapter 6, personal data must be protected against unlawful or unauthorized access or processing, accidental damage, destruction, or loss. Technical or organisational measures should be used to guarantee this protection.
- **Accountability**: The data controller must ensure that all previous principles are followed and that his or her company is compliant to them. Demonstrating this compliance is a requirement.

7.2. Lawfulness and Consent in the GDPR

Lawfulness of data processing and consent are two very important factors in the field of data protection, as stated in the GDPR [47]. As previously mentioned, lawfulness is not only optional, but one of the basic principles. There is only a limited number of reasons how processing can be lawful. The more obvious ones are processing in the name of the law, for contractual purposes or as a vital interest of individuals or the public. Moreover, the data controller can process data if the purpose is his own legitimate interest, as long as they do not exceed the interests of the individual. The safest way however is when a data subject consents to the processing of data for a set purpose. A data controller must be able to prove that a data subject consented to the processing of data. While consenting, the purpose and extent

of the consent must be clearly stated for the data subject and a withdrawal of consent must be possible at any time, which the data subject must be informed of. The GDPR states the age of 16 as a requirement for giving consent, but national implementations of the regulation can go as low as 13. In Austria, the age of consent for data processing is 14 [92] and therefore lower than what is specified in the GDPR. If necessary, the controller can demand proof for validating the age of a data subject. Freedom of expression and freedom of information are additional factors stated in the Austrian DSG, which can be used to determine a lawful processing of personal data. Additionally, the DSG states that every processing step must be logged in an appropriate way so that the lawfulness of the processing can be guaranteed and for reasons of traceability and auditability. Automated processing requires automated logging with at least timestamped information about the data at hand, the responsible person for the processing, identities of possible personal data recipients, and the processing purpose used to claim lawfulness. For systems that do not use automation, such protocols must include logs about rectification, erasure, disclosure and requests of personal information.

7.3. Special Categories of Personal Data in the GDPR

Special Categories of Personal Data, also known as sensitive personal identifiable information, is information that can be used to discriminate people or that provides a deep insight into a person's life, like medical conditions for example. The GDPR [47] prohibits the processing of such data, except for a number of reasons. Processing of such data is allowed when such a processing is needed to safeguard the rights and interest of the data subject, to fulfill contractual or juridical obligations that require processing of personal data, as a preventative measure concerning health or in case of substantial public interest, and for scientific purposes of course. Processing data of persons that cannot give consent is allowed when the processing is required to protect vital interests of natural persons. What organizations have to take into account is that the processing of special categories of personal data is no longer allowed with *legitimate interests* of the organization as a reason for the processing.

7.4. Rights of the Data Subject in the GDPR

The GDPR [47] specifies that providing and communicating relevant information is an obligation of the data controller. This includes the articles 13, 14, 34 and 15 to 22. Providing requested information is not required to be in written form, but it must be appropriate. This means that an information request can be

answered orally, if specifically requested by the data subject. When a data subject requests the exercise of data subject rights, the data controller must oblige as soon as the data subject has been identified. Any action taken shall be communicated to the data subject and action must be taken within one month of the initial request. If no action is taken, the data controller must inform the data subject about this non-action.

7.4.1. Articles 13 to 15 GDPR - Right to Information, and Access to Personal Data

Article 13 states that the information about where and what data is collected must be made available to the data subject. This information must be provided at the time of the collection. The information includes contact details of the data controller and the data protection officer, why and how the data will be processed regarding its legal basis and purpose, with an extra statement whether and where data processing is happening on the basis of legitimate interests and who the interested party is. Furthermore, it must be stated if there are any recipients of the data and whether is is intended to transfer personal data outside of the legal area of the GDPR. For the sake of transparency and fairness it is additionally required to state information about the intended storage period of the data. Adding to that, the data subject rights must be made clear to the data subject. This includes the right to erase, rectify or restrict personal data, withdrawal of consent and information about why it is important that personal data is collected. If there is automatic decision-making at play, the data subject must be informed about that as well. Finally, the data subject must be informed about the option to complain to a supervisory authority. The form in which this mass of information must be provided is not specified any further and therefore up to each organization. If personal data was collected from sources other than the data subject, the data subject must be informed about the collection and its circumstances. If a data subject desired to have access to information about the processing of affected personal data, this wish shall be granted by the data controller. Information of all categories stated above shall be included in the information provided to the data subject. This *Right of Access* can be limited however, if it would affect the "rights and freedoms of others". Additionally, if a data subject makes excessive demands, the controller can charge this information process accordingly [47]. Another restriction is formulated in the DSG [92], where access to personal information can be levered out to protect trade secrets of the data controller or a third party. It must be ensured however, that the data controller eases access to and informs a data subject about its rights and immediately inform a person in written form about what is planned to answer a data protection request.

7.4.2. Articles 16 to 20 GDPR - Right to Rectification, Erasure, Restriction, Notification Obligations and Data Portability

Collected personal data must be complete and accurate. It is therefore the right of a data subject to demand according rectification of stored personal data. If the accuracy of personal data or its lawful processing cannot be guaranteed, the data subject can demand a restriction of the personal data. This is also true for instances with uncertainty about the legitimacy of the processing of data, until a solution is found. Restricted data shall no longer be processed and only readable. If the status of affected restricted data changes, the data subject must be informed. When a data subject decides to withdraw consent or when there is no legal basis or legitimate interests for the processing of personal data, an erasure of the data must follow. The erasure of data can still be forestalled, if the personal data in question is needed for the compliance to laws and legal obligations, the exercise of rights, reasons of public interest, archiving purposes and for matters concerning legal claims. If a data subject makes use of any of the mentioned rights to *Rectification, Erasure, or Restriction*, the data controller must notify any recipient of the affected data if proportionally feasible and provide information about them, if required. Data subjects have the right to data portability, which means that a data controller must provide them with a commonly structured and ”machine-readable” format of the stored personal information so that it could be either simply handed over to the subject, or transferred to another data controller [47]. The Austrian DSG [92] states additionally that rectification or erasure of automatically processed personal data can be postponed if it would result in disproportionate efforts otherwise.

7.4.3. Articles 21 and 22 GDPR - Right to Object, Automated Decision-Making and Profiling

A data subject must be informed about the right to object the processing of personal data on the grounds of public or legitimate interest which then forces the data controller to prove that the processing of said personal data is legitimate and levers out the rights and interests of the data subject. If the objection is aimed towards direct marketing purposes, the processing must cease. Completely automated processing of personal data that is used for decision-making, including profiling, is generally not allowed according to the GDPR, with a number of exceptions. If such practices are required for the fulfillment of a contract, are allowed or required by law or are confirmed to with the consent of the data subject, an automatic processing and decision-making of personal data including profiling is lawful, if according measures are in place to protect the data subject and his or her rights, freedoms and legitimate interests. It is however necessary to ensure that human intervention into the decision-making process is possible [47].

7.5. Responsibilities of the Data Controller

With the collection of data comes great responsibility. This includes the implementation of adequate data protection measures. These technical and organizational measures shall be implemented according to the identified risks, context and purposes regarding the processing of data. Such measures must follow a continuous improvement process where they are reviewed, evaluated and kept up-to-date to the current threats and risks. Functioning data protection measures are a crucial element for the compliance of the data controller to the GDPR. The use of data protection policies is a way of implementing these measures [47]. Furthermore, the regulation states two additional manifestations for how data protection measures shall be implemented. Namely, to ensure *Data Protection by Design* and *Data Protection by Default*.

7.5.1. Data Protection and Privacy by Design and Default

Technical and organizational measures shall ensure that measures specifically designed to protect personal data, the data protection principles and the rights and freedoms of data subjects are in place [47]. Implementing technical security measures by design is a difficult tasks for many systems engineers according to [50]. There are many that lack the required knowledge about security and privacy specifics and therefore it is unclear what exactly a system should be able to do and not to do. To overcome that problem the authors suggest the introduction of a privacy engineer role so privacy by design can and will become more accessible and therefore adopted more adequately. To ease the implementation process for privacy by design requirements, the authors of [55] outlined seven principles and created a reference framework. According to these, to achieve privacy by design one must be proactive and preventative, see privacy as the default, embed privacy into the design of new technologies, maintain full functionality of a system, introduce a secure lifecycle end-to-end, introduce visibility and transparency, and respect the user's privacy. Another approach to privacy by design has been introduced by [56] and it is similar to classical information security, as it focuses on a series of protection goals with which technical and organizational system requirements are formulated. These goals include traditional information security protection goals like confidentiality, integrity and availability, but are also extended to include transparency, unlinkability, and intervenability. This extension of the traditional CIA-model is also explained in [94]. As with any form of regulation and requirements, there arise a number of challenges that need to be addressed [51]. First and foremost it is important to understand what exactly needs protection so it can be protected accordingly. Once that is achieved an organization can introduce a systematic privacy methodology with which systems are to be developed. This requires knowledge about possible risks so they can be addressed adequately.

Data protection by default is equally as important as data protection by design. According to the GDPR

this means that technical and organizational measures shall ensure that personal data is protected from processing by default [47]. This aims at ensuring that there must be a valid purpose for processing the data and to prevent an accidental processing of personal data [95]. This would empower a user to specifically and especially knowingly allow for advanced or more invasive processing of personal data instead of a user having to opt-out after the fact. Data protection and privacy by default becomes increasingly important in the context of social media and with cookies while browsing the internet. These are usually the main examples for invasive tracking and gathering of personal data to the disadvantage of the individuals.

7.5.2. Non-EU Processors and Third Parties

Although the GDPR is a regulation of the European Union, there are still specifications made for non-EU processors and countries. It is legally possible to become a processor for European data from the outside, but having a representative in one of the affected member states is a requirement. This is also relevant for organizations that want to use services from providers and processors of other parts of the world as an outside organization with an established representative is compliant to or on its way to being compliant to the GDPR. Third parties in general need to have organizational and technical measures implemented that are adequate for the purposes of and protection during the processing of personal data as stated in the GDPR. Data processing by third parties must be controlled with and specified in a contract that respects the requirements principles and rights stated in the regulation and it is the responsibility of the data controller to ensure that any third party has put adequate data protection measures in place [47].

7.5.3. Records of Processing Activities

Record keeping of the processing activities is mandatory for data controllers and processors. It is therefore of vital interest for organizations to create, maintain and store proper records. Fortunately, there are clear requirements for such records stated within the GDPR and the organization must be able to provide an electronic copy of this register to a supervisory authority if a request is made.[47]:

- Contact details and the name of a data protection officer and the data controller;
- Specification of the purpose why personal data is being processed;
- Category descriptions of data subjects;
- Category descriptions of personal data;
- Category of recipients of personal data;

- Data transfers to third countries and according documented protection measures;
- Expected storage duration per data category;
- General description of technical and organizational measures;

7.5.4. Data Security

The data security specifications stated in the General Data Protection Regulation [47] have a lot in common with information security practices, principles and measures, which have been described in more detail previously in chapter 6. The selection of appropriate technical and organizational data protection measures is based on a preliminary risk assessment and the state-of-the-art. Risks concerning an unlawful processing of personal data that infringes the rights and freedoms of individual persons must be highlighted and should be focused on in any evaluation of risks. Any measure that is to be implemented must consider these two factors concerning the rights and freedoms of data subjects. Furthermore, the regulation states that the information security principles of *confidentiality, integrity* and *availability* must be ensured. This shall be achieved, amongst other measures, by regular assessments and evaluations of implemented measures and a functioning incident handling process. If however a data breach occurs, the organization must inform a competent supervisory authority about the breach within 72 hours when the breach threatens the rights and freedoms of affected data subjects. The breach report must include information about the breach itself and how many persons are likely to be affected and what consequences these people have to fear, contact information for a point of contact (most likely a data protection officer), and all measures that are at play for the incident response process. If a data breach results leads to a severe threat to the rights and freedoms of a data subject, the organization must inform the affected natural person as soon as possible to explain the situation, provide contact information, expected consequences and active measures to protect the data subject. Informing the affected person becomes dispensable however if previous measures ensure that data affected by a breach is physically impossible to use in connection with the data subject because of i.e. encryption or the incident handling effectively eliminated the threat to the rights and freedoms of a data subject.

7.5.5. Data Protection Impact Assessment

Before starting to use or implement a new process or process operations that affects the rights and freedoms of a data subject, an organization shall conduct a *data protection impact assessment* prior to the first use of these operations and processes [47]. Such an assessment is not a direct responsibility of a data protection officer, but at the least his or her opinions and concerns should be included and

respected. Additionally, a data protection officer can give advice to the overall responsible data controller. A supervisory authority can specify certain areas or processing operations that require a data protection impact assessment. If none of the specified processing operations are implemented within an organization, an impact assessment must be conducted nonetheless if the processing operation includes automatic processing or profiling as a basis for decision-making or personal information of special categories. Any data protection impact assessment must at least include information about *the processing and what purpose it serves, whether the intended processing is still within the limits of achieving the specified purpose, how the processing affects the rights and freedoms of a data subject, whether there is a legitimate interest of the organization at play and its relation to legitimate interests of the data subject regarding a lawful processing and compliance to the GDPR* and especially *which security and protection measures the organization has intended to protect both the individual and his or her personal data*. Any impact assessment should be reviewed at regular intervals or with any changes to the intended processing operations or with a changing threat and risk landscape.

7.5.6. Data Protection Officer

As the name already suggests, a data protection officer plays an important role for data controllers and processors, with some of the most important underlying fundamentals and tasks specified in the GDPR [47]. Appointing a data protection officer (DPO) is mostly relevant, or even obligatory for public authorities, and for organizations that either systematically monitor data subjects, as well as for organizations that process sensitive personal information on a large scale as one of the primary undertakings of the organizations. It is not however necessary that a DPO gets appointed within an organization. That role can equally be fulfilled by a contractual partner. What counts are the qualifications and professional experiences of a person. Once someone is assigned to the role of a data protection officer, his or her contact details shall be communicated accordingly, including informing the supervisory data protection authority. Even if it is not a legal obligation for an organization to hire a data protection officer, it can be highly beneficial nonetheless [96]. A DPO will continuously guide the organization to be compliant to the regulation as the mere fact of such an appointment will help demonstrating the will and accountability of an organization and data protection efforts will be more effective if advice from such an officer is taken seriously. This in turn will help to meet various requirements of the regulation much easier and especially in a more organized fashion which makes it better suited for future changes and to set up a future proof data protection policy. However, for most smaller organizations it will be more likely to hire an external data protection officer.

Once the role of the data protection officer is established in an organization, there are a number of re-

quirements, tasks and obligations that come with it [47]. For one, it is not enough to merely appoint a DPO. He or she must also be involved appropriately in any data protection matters. Additionally, management support is an important factor. If the needed resources to properly conduct data protection activities are not provided by an organization, there is nothing a data protection officer can do. Likewise it is important that a data protection officer can perform the required activities undisturbed and conflicted and is only required to report to the highest levels of management. Furthermore, a data protection officer will most likely become the first point of contact for any data subject with concerns regarding data protection. There are five specific tasks of a DPO mentioned in the GDPR, which he or she must perform with underlying risks in mind:

1. Internal guidance and informing about regulatory obligations concerning the processing of personal data;
2. Monitoring of compliance to the regulation, national laws, internal policies and other obligations concerning data protections, as well as performing training and awareness activities where needed;
3. Support the effectiveness of data protection impact assessments and provide needed information and advice;
4. Work openly and cooperatively with supervisory data protection authorities;
5. Take care of data protection obligations regarding the communication with and reporting to supervisory authorities concerning the processing of personal data, especially when there is an obligation to inform;

The DSG [92] expresses an additional obligations. Namely, a data protection officer has the obligation of secrecy, especially about identities of data subjects. This provision is extended to also include other people that work with personal data like the data controller, a data processor and even employees. It also includes the transmission of personal data in a way so that a direct order of the employer is needed for an employee.

7.5.7. Image Processing

In the Austrian Data Protection Law [92], image processing and its lawfulness is specified, contrary to the General Data Protection Regulation. This includes pictures and especially videos. Lawfulness for image processing has similar requirements as any other form of data processing, namely vital and lawful interest, consent or on basis of a legal requirement. For video recordings with surveillance cameras it must be ensured that they are solely directed on private property and do not capture any public areas.

There are of course exceptions to this rule. Furthermore, video footage should not be stored for a period longer than 72 hours, unless there is a proportionate reason and it is done separately from regular recordings. Additionally, any recording must be labeled accordingly if there is a regular processing of such material at hand.

7.6. Privacy Information Management System - PIMS

As already mentioned in chapter 6, the ISO 27001 is a cornerstone of information security and especially information security management systems. Considering the importance of a functioning management system for an improvement of quality and especially to prove said quality, a management system for data protection and privacy is desirable, although not explicitly required according to the GDPR. When the GDPR came into force, the lack of existing standardization opened the path for many organizations to develop and offer their own version of a data protection or privacy management system of which many clearly follow the overarching ideas of the ISO 27001 and its ISMS [97, 98, 99]. One model highlights the importance of and centers around the idea of the PDCA-Cycle as the driving factor of the management system [97]. Their idea of implementing a *Data Protection Management System* (DPMS) includes data protection guidelines, review processes for data subject requests, awareness and training programs, technical and organizational measures, the appointment of a data protection officer and a data classification. A different model proposed by [99] is presented as a two-step-model. Step one focuses on the preparation and implementation of a DPMS and what is needed for its very foundation. The second step involves operation and continuous development of the system. In [98], they present yet another approach. They propose a Data Protection Management System on the basis of the COBIT framework with a strong focus on process oriented data protection. Highlights of their program are the inventorisation of data and the creation of data maps and the creation and management of records concerning data subject requests, relevant measures and consent.

All of the mentioned approaches are equally valid for becoming compliant to the requirements of the GDPR. For organizations that already have an existing management system in place or the ones that plan on introducing more than one management system, it is advisable to integrate both systems. One way to integrate data protection and privacy to an information security management system based on the ISO 27001 is following the guidelines of the ISO 27701, which focuses on the implementation, maintenance and continuous improvement of a *Privacy Information Management System* (PIMS), which enhances the ISO 27001 controls and specifications by a set of privacy specific counterparts [100]. A large portion of technical and organizational security measures required by the ISO 27001 will already ensure compliance to these specific parts of the GDPR, the same is valid for other parts i.e. the assessment

and mitigation of risks. Specifics for personal information are however not addressed. However, with the guidelines described in the ISO 27701, full compliance to the GDPR is no longer wishful thinking as they now can address both classical information security and data protection requirements with one unified system.[101, 102]. Additionally, combining these two systems will also allow for a certified ”proof” of data protection compliance via the ISO 27001, which is otherwise not yet possible for data protection and privacy specifically, as a specific standard to certify against does not exist at the time of writing. The ISO 27701 specifies where additional requirements would be needed, to make the ISO 27001 clauses GDPR-compliant, which can be seen in the following table 7.1.

Clause in ISO/IEC 27001:2013	Title	Subclause in this document	Remarks
4	Context of the organization	5.2	Additional requirements
5	Leadership	5.3	No PIMS-specific requirements
6	Planning	5.4	Additional requirements
7	Support	5.5	No PIMS-specific requirements
8	Operation	5.6	No PIMS-specific requirements
9	Performance evaluation	5.7	No PIMS-specific requirements
10	Improvement	5.8	No PIMS-specific requirements

Figure 7.1.: Location of PIMS-specific requirements and other information for implementing controls in ISO/IEC 27001:2013 [102].

As clearly visible, there are only two clauses of the ISO 27001 that need to be enhanced with privacy specific requirements. Additional guidance with a focus on privacy is however more present when conjunct with the ISO 27002. There the only clause that does not require additional PIMS-specific requirements is clause 17, business continuity management. Additionally, the ISO 27701 defines a set of privacy controls in its Annex, that can be used as a guideline to become data protection compliant for both controllers and processors of personal information.

7.7. Data Protection Documentation and Records

This section will summarize the required and recommended documentation and records which are necessary for the implementation, operation and improvement of data protection within an organization. This includes templates that could prove themselves useful during incidents. The following checklist is provided as a guideline tool for organizations seeking to implement required data protection and privacy systems.

- ☐ Public privacy statement and data protection policy

- ☐ Information about the rights of a data subject and processing activities to comply to the *obligation to notify*, which shall include the following:
  - ☐ Contact details of the data controller
  - ☐ Contact details of the data protection officer, if appointed
  - ☐ Type of personal data that will be processed
  - ☐ Purpose of the processing
  - ☐ Whether the data will be transmitted to third parties
  - ☐ Expected storage duration of the personal data
  - ☐ Information about the data subject rights, including the right to withdraw consent and the right to complain to a supervisory authority
- ☐ Records of processing activities
- ☐ Risk and data protection impact assessments for the high risk processing of personal information
- ☐ Records of technical and organizational measures and according training courses
- ☐ Contact details of the data protection officer being made public and reported to the supervisory authority
- ☐ Records of the declarations of obligations of employees
- ☐ Records of data protection training programs
- ☐ Records of the declarations of consent of customers

Part III.

Design Thinking Framework for Information Security and Data Protection

8. Combining Design Thinking with Information Security and Data Protection

This chapter will discuss elements of Design Thinking, information security, and data protection in regard for possible compatibility between them. Areas of high congruence would prove ideal for combining these different fields, as without any similarities, the creation of any combined framework can become difficult. Likewise it is important to highlight such incompatibilities so that expectations are realistic and a framework is not seen as a lucky back that can do everything, but rather to become aware of its strengths and weaknesses to act accordingly.

8.1. Harmonizing Design Thinking and Information Security/Data Protection

Continuity & Continuous Improvement In both Design Thinking and information security there are elements of continuity. In information security it comes in the form of continual improvement (6.3.1) of both the controlled systems and the structured approach on information security itself. In Design Thinking forms of continuity can be found in i.e. a design sprint (5.6), and the idea that design work never stops, as there will always be ways to improve a product or customer experience as a result of iterative processes.

In information security, the go-to model for the establishment of an ISMS and its continuous improvement is a PDCA-Model (6.4). When compared to the Design Thinking micro process (5.3), there is a resemblance of similarity between some of the steps. The first element of the PDCA model, *Plan*, can be compared to the steps *Needfinding & Synthesis, and Ideate*. It is here where problems/risks are identified and understood/assessed. Additionally, The planning phase is technically similar to the *ideate* step, as both try to come up with solutions on how to best implement their respective goals based on the preliminary assessments, evaluation and gathered information. The *Do* phase of the PDCA is strikingly similar to the *Prototype* step, as both of these are concerned with the implementation of what had been previously planned and imagined. *Check* and *Test* are again congruent, as both will evaluate and review

what has been implemented. The last phase of the PDCA, *Act*, and the remaining step of the Stanford micro process, *(Re)define the problem*, are again focusing on the same aspect, continuous improvement and a never-ending cycle.
It can therefore be said that the aspect of continuity, especially on the process level, is not only present in both Design Thinking and information security, it is also handled in a very similar manner. In the field of data protection, the concept of continuous improvement does not have the same significance as in the other two. That is not to say that it does not benefit from it. This has been highlighted in 7.6.

Risk Assessments Risk assessment and a risk-based approach is an important part of information security, and specifically of an ISMS (6.3.2). Likewise the importance of according risk mitigations and controls can only be highlighted once more. Design Thinking on the other hand does not follow a risk-based approach. Instead the focus lies on the customer and his or her needs. As pointed out by [103], the iterative approach of Design Thinking with its strong customer focus will ensure that the result is closer to what was expected and therefore the risk of a failed product, project or service is substantially reduced. Such an iterative approach of Design Thinking is the core concept of *Design Sprints* (5.6).
At first this seems like an incompatibility, because addressing risks directly is still completely different from a passive risk reduction as a result of iterative improvement. There is still hope however, as pointed out by [104]. Risk management can be conducted by using a Design Thinking framework. It is pointed out how the steps of a basic Design Thinking process (Empathise, Define, Ideate, Prototype, Test) can be used to directly practice risk management. These claims are underlined with examples on what each of the steps can and will do for the risk management of an organization. Since it is a rather different approach on the matter, it might be a viable alternative for organizations that struggle with traditional risk management.

Customer-Oriented Processes With Design Thinking focusing heavily on empathy and how problems can be solved with a customer-centric view, it comes to no surprise that it can be used for information security and data protection as well. For information security, the Design Thinking approach can be used to understand stakeholders better and to provide more streamlined security processes to the employees. The same is true for the field of data protection. Especially in case of direct communication with a customer. For example, the regulation requires that if a data subject requests information about stored personal data, the organization storing them must deliver the information in an appropriate form and in a timely manner (7.4). Using Design Thinking to create a process to not only deliver the requested information, but also doing it in a way that a customer will approve of can improve public opinion. Service Design Thinking can elevate the overall quality of delivered IT-services, whether internal or external.

Resources Having the right and especially sufficient resources is focused on in all categories. The importance of resources in Design Thinking has been mentioned in this thesis already (3.2). Without having the right rooms, tools, materials, people involved and testing, and to some extent even skills, it becomes harder to conduct successful Design Thinking processes. Likewise in Information Security and Data Protection, you have to have certain resources or else it becomes virtually impossible to implement safeguards, security measures, or spread awareness about certain issues. Having the right resources and competencies even becomes a mandatory requirement for management systems, as described in various ISO standards [84, 41, 80, 102].

8.2. Incompatibilities of Design Thinking and Information Security/Data Protection

Writing Documentation While written documentation is a cornerstone of information security and data protection, especially for organizations that aspire to get a certified ISMS implemented, it is not feasible to achieve it with Design Thinking techniques. Design Thinking could be used to frame certain documents or to generate basic concepts of policies and instructions. In the end however, no amount of brainstorming and design sprinting will spare the necessity of having to sit down and write these documents. It is virtually impossible to only use Design Thinking tools and expect a fully implemented, holistic, and standard-compliant documentation as a direct result.

Laws and Regulatory Requirements Similar to the previous point, when a law demands a certain piece of information or system implementation, there is no way to ”design think” a solution for that. Specifically speaking, if an organization is requires by law to implement state-of-the-art encryption on its systems, it is a definitive statement. This can equally be valid for business contracts and other frameworks. Overall it is therefore highly unlikely to use Design Thinking as a universal tool for all business processes and operations.

9. SecDT-Framework

In this chapter the conclusions and acquired knowledge of the previous chapters will be used to collaborate with a partnered organization where the aim is to introduce elements of information security and data protection by using Design Thinking methods. During this collaboration, the direction of this work will be geared to the needs and problems of the partner organization as there are so far no previous implementations for information security or data protection of any kind. It is therefore a clean slate, which will be considered for the introduction of new specialist topics.
This chapter will begin with presenting a proposed framework that combines Design Thinking with information security and data protection. After a short explanation of the framework elements and rationale, the partner organization is introduced. This is followed by a display of a workshop that is meant to mimic elements of the framework and to present the subjects of this thesis to the partner organization.

9.1. Structure of the Framework

The proposed SecDT-Framework (Security Design Thinking Framework) for combining Design Thinking with Information Security and Data Protection, as seen in figure 9.1, is comprised of various elements that should be familiar to practitioners of both worlds. Each of the elements will be described in this section.

Input - Problem The input is what drives the whole framework. It is here where requirements of various kinds, objectives, needs of stakeholders, and further propelling forces enter the system. An initial and rough *problem statement* that describes the starting situation or position is sufficient at this point. There is no need for fully specified procedures, but rather pointing to a general direction to know what should be solved.

Output - Solution The Output, or Solution or the framework is a general approach on how to each an objective, or an expected result of the process. This could be the establishment of a whole ISMS, the implementation of a single process, refining of existing components and procedures, or anything that is

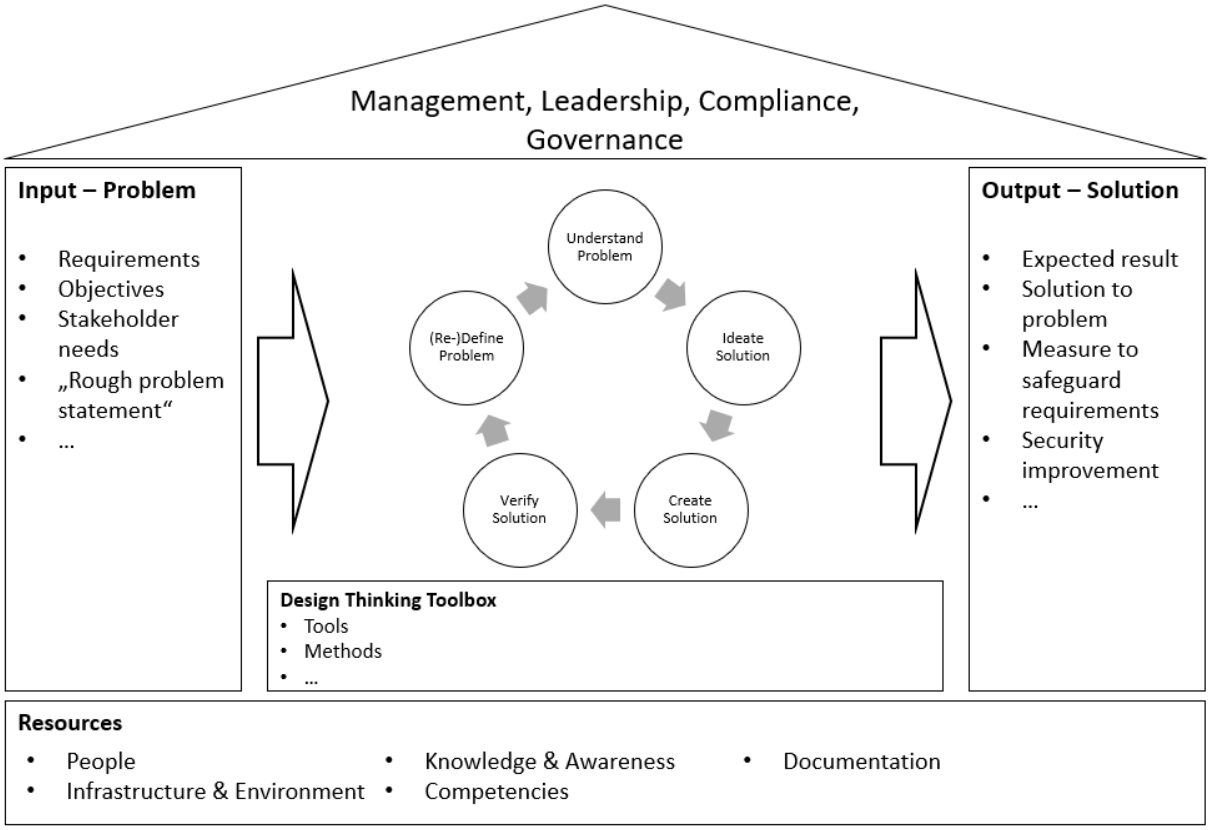


Figure 9.1.: Proposed SecDT-Framework

meant to improve the overall levels of information security and privacy within an organization.

Problem-Solution-Process This is the element where the heart of Design Thinking practices lies. A *Problem-Solution-Process*, oriented on different Design Thinking process models described in chapter 5. It gets a problem as input and is meant to deliver a solution to that problem. This becomes even more apparent when looking at the components of this process. It can be generally split into two spaces, the *problem space* and the *solution space*. The solution provided in such a process is experimental at first and will only become a registered measure once it is verified successfully. The individual phases of this process are the following:

- **(Re-)Define Problem:** The initial problem statement that serves as the input is analysed even further. The rough formulation is taken and specified to become an unmistakable question, rather than just the rough idea of a problem or requirement. A clear definition of what the specific problem actually is and means to the organization is the needed foundation for the following phases.
- **Understand Problem:** Once there is a clear and refined problem statement, it is now time to dig deeper into the problem. It is a phase of analysis and information gathering to understand the

extent of the problem and the stakeholders involved. This does not only include the initial problem statement, but also the underlying components and causes of said problem. The root causes so to speak.

- **Ideate Solution:** Once it is clear what the problems are, what causes them and what their effects are, it is time to find solutions to the problem. This can be done in a brainstorming session or by other means. The important part is that ideas are generated quantitatively so that there is a large pool of ideas available.
- **Create Solution:** After generating ideas for the problem, it is now time to assess these ideas. Not all ideas will have the same effect or impact on an organization and others might even become money sinks. Especially for organizations with limited resources it is vital that presented ideas are selected carefully. After the selection process for the most valuable ideas, they have to be implemented. In Design Thinking that means experimenting. The results created here are the output of the process.
- **Verify Solution:** The experimental implementations of solutions will be verified. If a solution solves the problem, it shall be documented accordingly. If a solution does not solve the problem, the whole cycle starts anew and the initial problem statement is re-defined. It is therefore, as the name suggests, a verification of what has been implemented. If the solution does not fully solve the initial problem, it can either be modified or the entire process can start anew with an additional problem definition.

Supporting Design Thinking Toolbox For the *Problem-Solution-Process* to function properly, it is important to have everything that's needed at the ready. This means a catalogue of fitting Design Thinking techniques and tools that are needed in each of the phases of the process. This can be an "off-the-shelf" toolbox like the *75 Tools for Creative Thinking* [105], or the *Mitre Innovation Toolkit* [68]. An equally valid approach would be to craft a completely separate toolbox or catalogue with tools and techniques that have proven themselves to be highly compatible with the workflows and mindset of the organization. It is not required to use all available tools for each individual process iteration. Only the ones that are the most suited to take on the task at hand.

Resources As already mentioned in the previous chapter (8.1), the availability of the right and needed resources is fundamental for the success of any Design Thinking, information security or data protection efforts. This includes *People, Infrastructure, Environments, Materials, Knowledge, Skills and Competencies, Awareness, Communication*, and of course *documented information*.

Management Management commitment, Leadership, Compliance, and Governance. These are all terms that anyone dealing with information security should be familiar with. Without the support of the management, all efforts and measures being implemented are reduced to a mere ”nice-to-have” without clear commitment from the top management of an organization. Especially when it comes to reporting, it is the top management that is being reported to. So their involvement is inevitable. It is also them who are responsible for providing needed resources and supporting the success. So it is their protective hand that is needed to receive a useful and positive outcome. Especially when an organized system or framework is being used.

9.2. Context of the Partner Organization

The partner organization for this experiment is a young and dynamic startup focusing on modern means of education and individual encouragement. Their main emphasis lies on mathematics, as it is one of the subjects at school that most children have a problem with. Their approach is a different way of introducing these topics, which are often times taught in an overly complicated way in regular school that only worsens the situation, and make it more accessible and easy to understand. Additionally, they want to promote the idea of seeing the value of mathematics as part of future career paths. Their formula is to teach mathematics in an interactive way that uses real world problems for its solution path and to answer the question ”Why do I need to learn mathematics?”. This and much more will be tackled by their smartphone application, in which modern technologies like AR are used for further facilitation of the topics.

Experiment Participants The three founding members of the organization accepted that their startup and they themselves will partake in the following experiment which includes a first iteration of the SecDT-Framework. Their current positions within the company are CEO, CTO, and COO, which allows for fundamental insights into the major realms of the organizations.

9.3. Experiment

In this section, an experimental iteration of the framework is presented. This is used to test the feasibility of the framework itself and the compatibility of Design Thinking with information security and data protection. All levels of management of the partner organization are included in this experiment, as it lies in their own interest to become aware of security and privacy issues, as well as how to effectively combat them.

Scope of the Experiment Since the creation or implementation of a complete ISMS or PIMS is neither feasible, nor possible as part of this thesis with the resources at hand, the scope had to be reduced to a more experimental nature and should thus be seen as a Proof-of-Concept, rather than an accomplished fact. The focus of this experimental framework iteration will be in line with the most pressing issues and requirements of the partner organization.

Input - Problem The initial problem statement comes in the form of a general approach. Since there are currently no security measures or safeguards implemented in the organization and the knowledge about information security and data protection is rather limited, getting to know the subject and existing problems becomes the point to start from. So the input problem for the experiment iteration is the desire to learn about existing issues, how the organization as a whole might be affected by them and what could be done to mitigate these problems.

Output - Solution The solution or expected output is therefore a proposed plan about how identified issues could be addressed. Especially data protection and privacy issues are a big concern for the organizations and solutions to such problems are therefore welcomed the most.

Problem-Solution-Process For this iteration the input (learning about existing issues and problems), is used as a starting point for this process. The end result of the process, the output so to say is the creation of an action plan for safeguarding the organization. What is done in the individual process steps is described below:

- **(Re-)Define Problem:** Since the input is only pointing to a general direction, it is now time to formulate a specific question for the process. To get to such a question, the ”How Might We”-Method [106] is used, where an initial problem is rephrased as ”How Might We”-Question. Since the initial problem is that security and privacy are practically non-existing, and knowledge and resources are limited, the question will be formulated in a way to encapsulate these challenges: *How might we identify and protect against the most pressing issues of information security and data protection?*
- **Understand Problem:** A workshop (9.4) will be held to cover this step.
- **Ideate Solution:** A workshop (9.4) will be held to cover this step.
- **Create Solution:** A workshop (9.4) will be held to cover this step.

- **Verify Solution:** A set of success criteria will be defined for the measures during the workshop (9.4). Once the action plan has been implemented properly and the measures had sufficient time to be evaluated, it can be assessed whether the success criteria have been satisfied or if there is need for an additional process cycle or a change of the initial problem statement.

Supporting Design Thinking Toolbox The Design Thinking tools used in this process iteration are a combination of tools described in chapter 4, as well as further additions from [105], [68], and [107]. Additionally, the online tool Miro [65] was used to have a canvas for visualization and cooperative work.

9.4. Workshop

The cooperation will kick-off with a workshop about information security and data protection. The workshop will be structured following the principles of Design Thinking work as outlined in *The Workshopper Playbook* where creative methods for successful workshops are described [107]. After the initial introduction, the workshop will be split into the four phases *Collect, Choose, Create,* and *Commit*. Each of these phases will utilize Design Thinking techniques to facilitate the complex subjects of information security and privacy. The expected result of this workshop is the creation of an action plan for safeguarding information security and data protection. The schedule of this workshop can be seen in figure 9.2.

To ensure that the workshop can be conducted with maximum efficiency, the online tool *Miro* [65] was used to prepare a work space for each task beforehand. A preparation of all needed tools and contents will help with reducing possible interruptions and uncertainties. These prepared ”whiteboards” can be seen in figure 9.3. The content of each task, the rationale behind it and the results will be described in the following paragraphs.

Before starting with the first phase however, the introductory block takes place. This includes a short introduction to this thesis for those who have not yet had contact with the topic, then an overview of the key elements of information security and data protection, so that all participants have the most basic needed understanding to tackle the tasks that wait before them. Additionally, we will assess the current situation about the state of information security and data protection within the organization. For this a SWOT-Analysis will be used with the focus on information security and data protection.

At first it felt a bit odd for the participants to do a SWOT-Analysis with a focus on a topic that they themselves are not overly familiar with. Especially the lack of strengths compared to the amount of weaknesses and threats worked like an eye-opener to show them how little there actually is and what the consequences of that could be. Although this exercise was still on a rather high level of observation, it

Figure 9.2.: Workshop schedule

helped a lot to understand the state of the current security levels within the organization. Additionally, it was already here in the first warm-up task that the participants identified proper information security and data protection handling as an opportunity for a competitive advantage. The SWOT-Analysis can be seen in figure 9.4.

9.4.1. Collect

The *Collect* phase is the first one of the described workshop phases in [107]. In this phase the focus is on collecting information and data, challenges, and problems in a quantitative manner. At the end of the phase the gathered information should be visualized for an easier understanding.

The first task of this phase will be a brainstorming session. By identifying the stakeholders, addressing their needs and issues becomes possible. This identification will be done in the form of a brainstorming

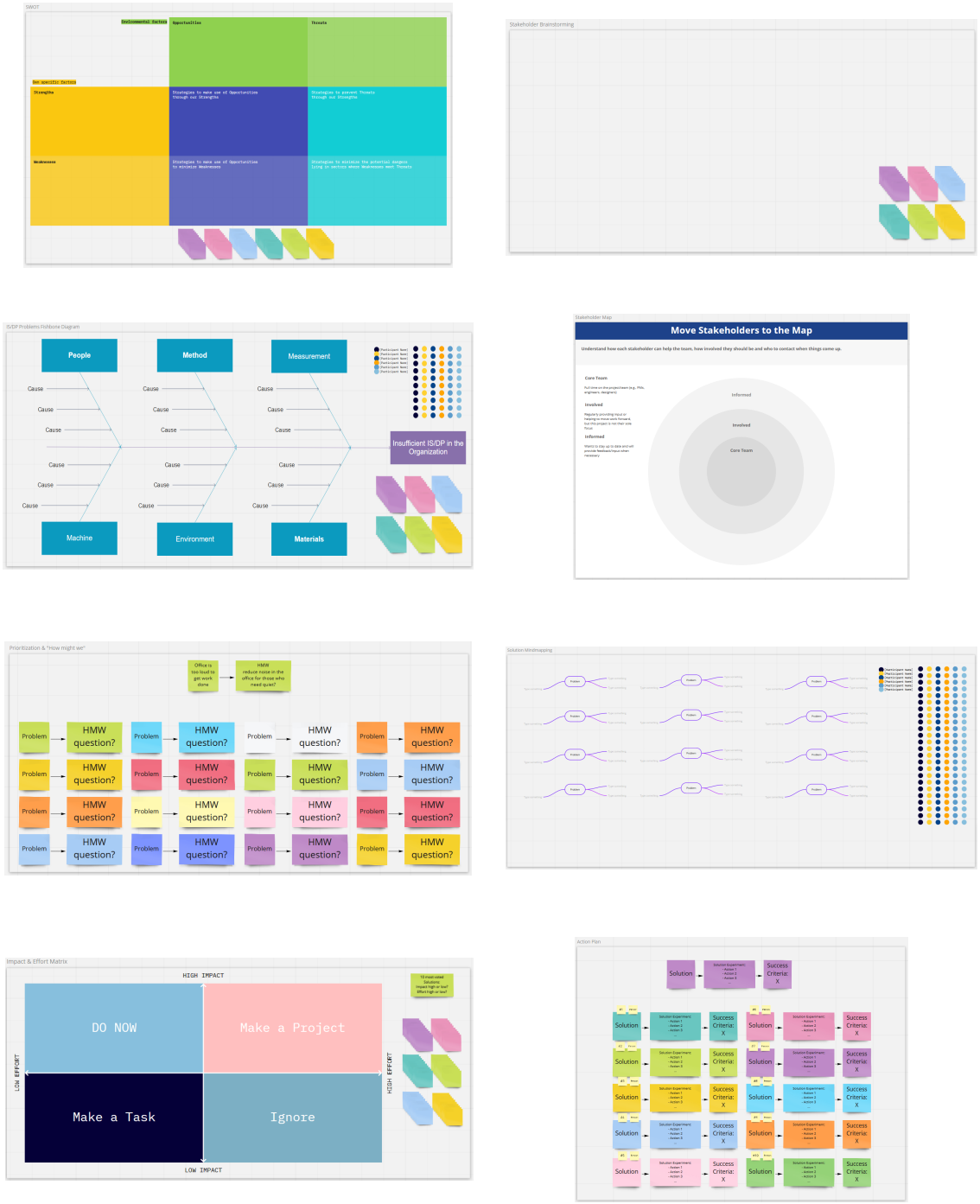


Figure 9.3.: Prepared ”whiteboard” work spaces for the workshop

to remove any possible obstacles that could arise by trying to categorize them or by trying to establish relations between the individual nodes. While an analysis of possible stakeholders is usually something that any organization does quite early in its evolution, this task was specifically chosen to highlight not only any interested parties, but also to show the partner organization how some of these might be affected

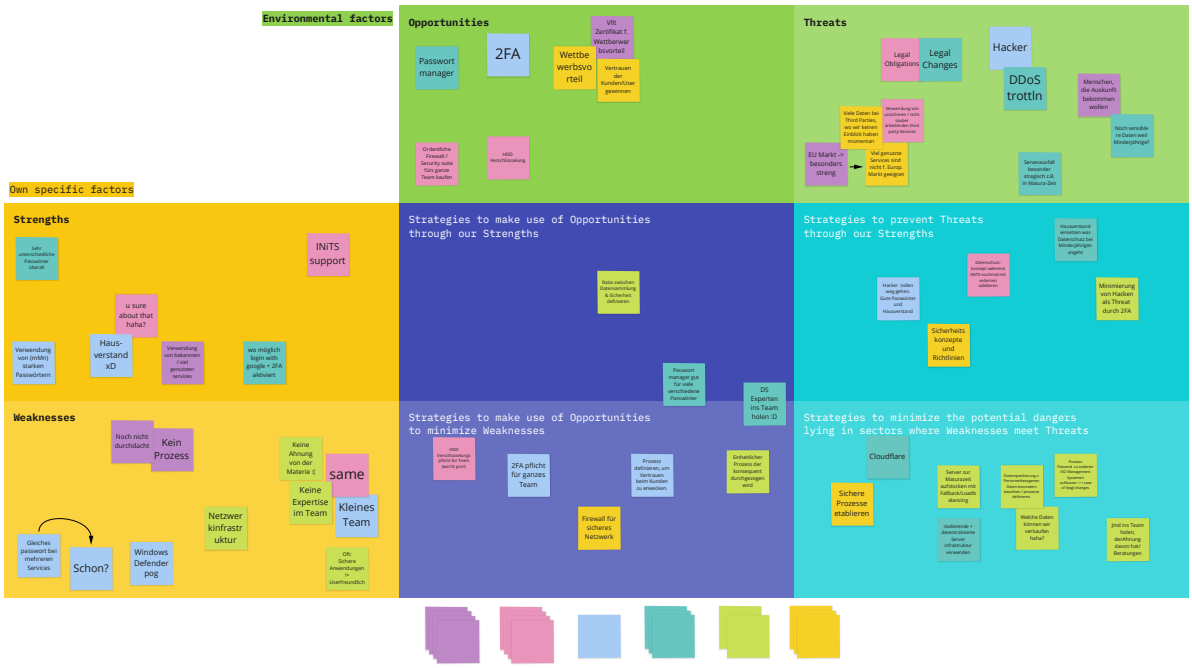


Figure 9.4.: SWOT-Analysis with a focus on information security and data protection

by their own implementations of security safeguards or the lack thereof.

While the participants had analysed stakeholders in the past already, the task of considering stakeholders based on information security and data protection helped to reveal several notes that were previously never thought about. Especially since there are multiple ”productivity tools” in use where there has never been a check whether these are even fit for use in the European Union or Austria. Most of these tools focus on a US market and therefore have a certain stance on privacy issues that might not be in the best interest of neither the partner organization, nor its stakeholders. Besides the identification of possible business partners or innovation hubs, a large portion of all notes during that brainstorming was centering around data protection and privacy concerns or considerations, as well as legal requirements imposed by the state. The brainstorming ”whiteboard” is included as figure 9.5.

The second task is a *fishbone diagram* [108]. The focus of this diagram will be the determination of various causes for the overall effect of dealing insufficiently with information security and data protection. Analysing these issues and especially the domains of them will be of great value for further processes. If for example one of the domains contains multiple and more severe causes, it might be a good idea to focus on this single branch specifically.

While the previous tasks were mostly to get a better understanding of the organization and its positioning, and to familiarize the partner organization with the topics information security and privacy, the fishbone

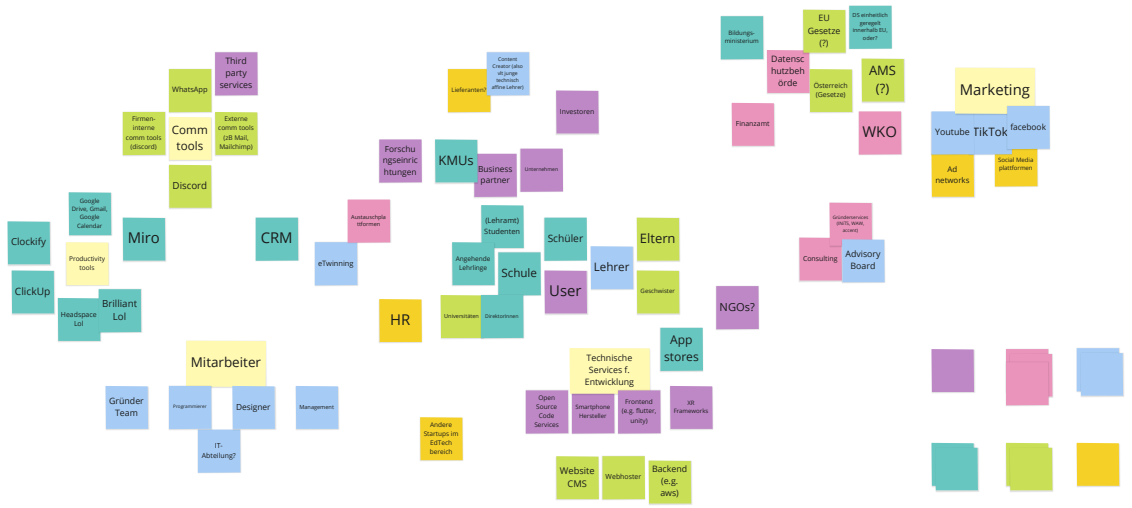


Figure 9.5.: Brainstorming about Stakeholders

diagram will unearth the most obvious causes that are leading to the overall state of insufficient information security and data protection handling within the organization. Working with this diagram was well received, because this type of root cause analysis with chained causes that lead to an ultimate negative result was something that they had never done before. However, some of the categories proved to be a hurdle, as the lack of knowledge about both IS/DP and the technical causes behind it made it difficult to find specific causes or to chain them. The domains that the organization was already familiar with however were quickly filled without any difficulties. This shows that it would be highly beneficial to include at least one person knowledgeable for each domains. Nonetheless, each of the domains harbored plenty of different causes or chained causes in the end. Figure 9.6 shows these causes, but also includes the dots of the *Dot Voting* process of the next phase.

9.4.2. Choose

This phase is used to filter all identified problems and focus on what the most pressing issues are. It is important that this phase is not used for introducing new ideas or problems. The sole purpose lies on narrowing the previous results down [107].

Since stakeholders have been identified already, they can now be properly mapped. A *Stakeholder Map* [68] will be used for this task. It consists of the three spaces *Core Team, Involved*, and *Informed*. These spaces help to divide all stakeholders based on their degree of involvement with the organization. It is also used to visualize relations between different stakeholders.

Structuring the identified stakeholders of the previous phase on a map like this was welcomed by the

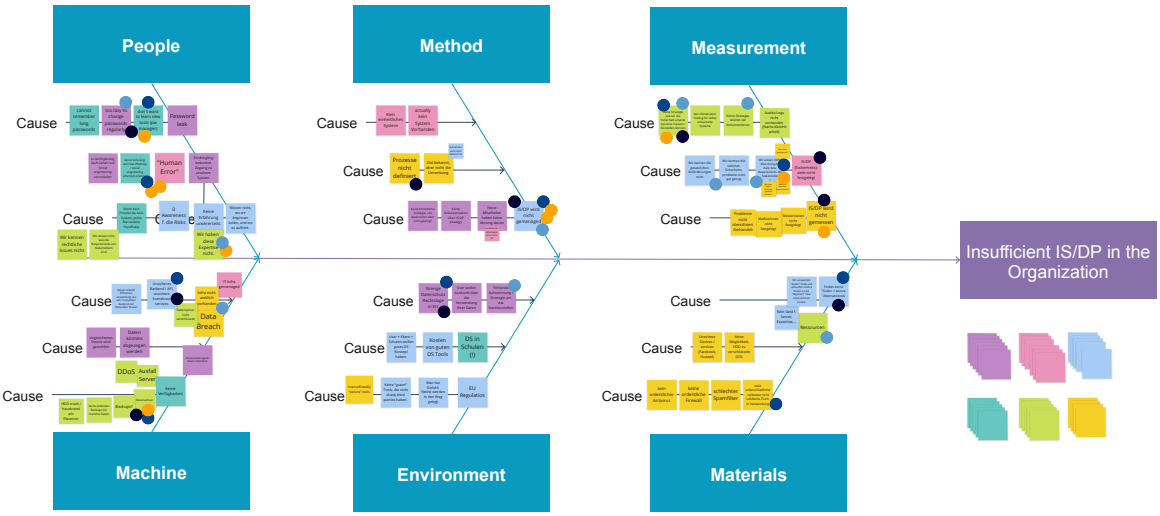


Figure 9.6.: Fishbone Diagram of the causes that lead to insufficient IS/DP in the organization

partner organization. By placing them based on their degree of involvement it showed quite clearly where there might be a lack of skills in the core team because. Additionally, it showed that some of the stakeholders that might appeared important before are actually only a minor concern for the organization. The distribution of stakeholders is shown in figure 9.7.

The last task of this phase will be the prioritization of the most pressing information security and data protection issues that have been identified by using the fishbone diagram of the previous phase. The prioritization process starts with *Dot Voting*, where all participants use dots to ”vote” what they think are the most important issues. Once all the dots are spent the next step is the actual prioritization where the 10 issues with the most votes will be taken to the next step, while the other issues remain where they are for now. These 10 most pressing issues will then be ”re-designed” to formulate a *How might we* question. This technique allows a problem that might still be rather abstract at this point to become a statement that specifically calls out the problem and what it affects in a way that the question itself already appears suggestive for a possible solution [106].

During the Dot Voting, each of the causes received votes ranging from zero to six. Out of all these we prioritized eleven causes to become the core problems for the next step, the *How might we* questions. All eleven problems were split so that each participant had a roughly equal amount of problems to deal with, then they were tasked with the creation of these questions where they included what needs to be done and why. The immediate feedback to this task was very positive, as this ”in-depth” engaging with the problem was beneficial for a proper understanding of the problem and leaving the high-level point of view behind. Even problems that are rather technical were no longer an obscure element. These

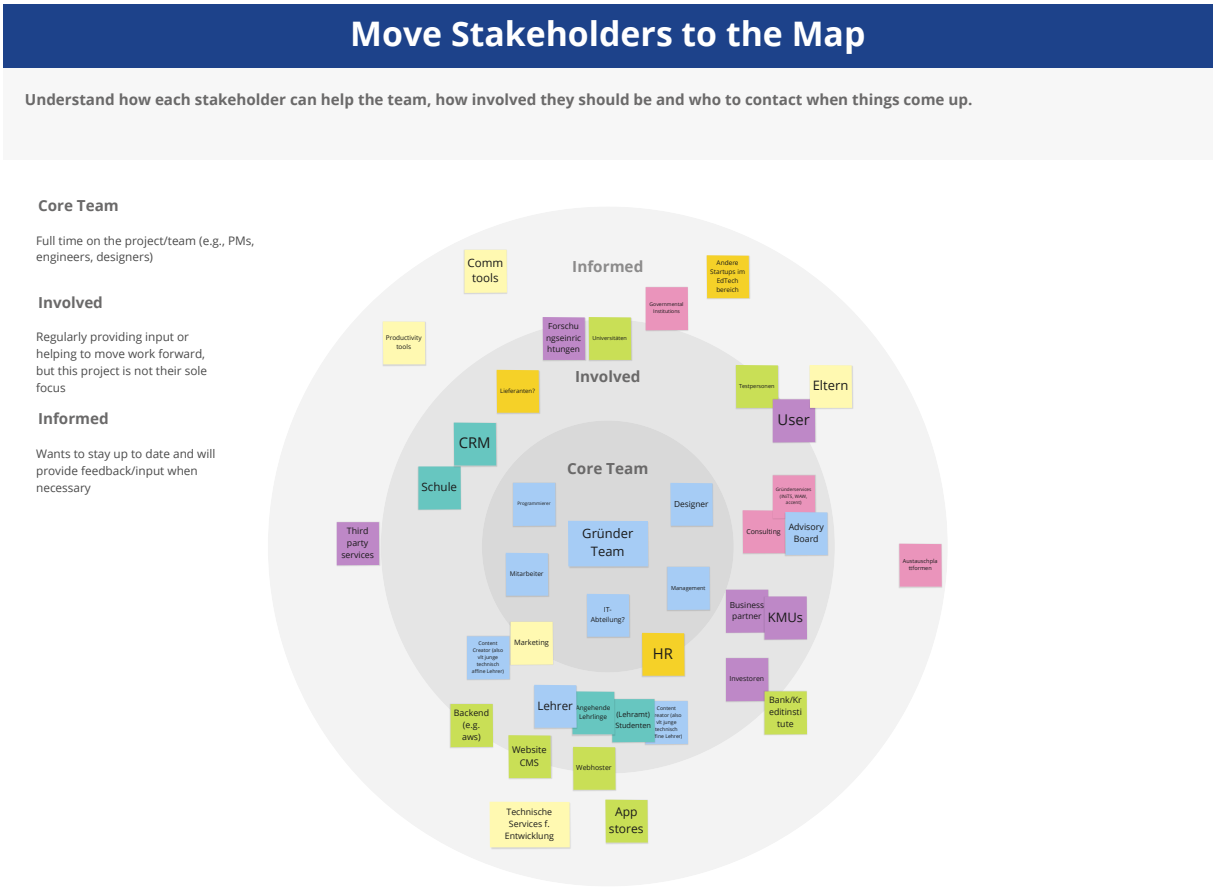


Figure 9.7.: Stakeholder Map based on the degree of involvement

HMW-questions can be seen in figure 9.8.

9.4.3. Create

During the *Create* phase, possible solutions and ideas on how to solve the previously identified and prioritized problems. Ideas that have been generated must be assessed and weighted to detect the most viable solution to a problem [107].

The planned task of the *Solution Space* is mind-mapping the previously defined ”How might we” questions as the core problem. The focus of the task is to generate as many possible solutions to the problem as possible. In the end, there will be another Dot Voting for each of the problems individually, to find the most valuable and viable solutions to each of the problems.

The result of this stage can be seen in figure 9.9. To ensure an equal distribution of solutions and to prevent participants being stuck on one single problem, the solution generation process was arranged as a round robin process where each participant was only allowed to write one solution suggestion for

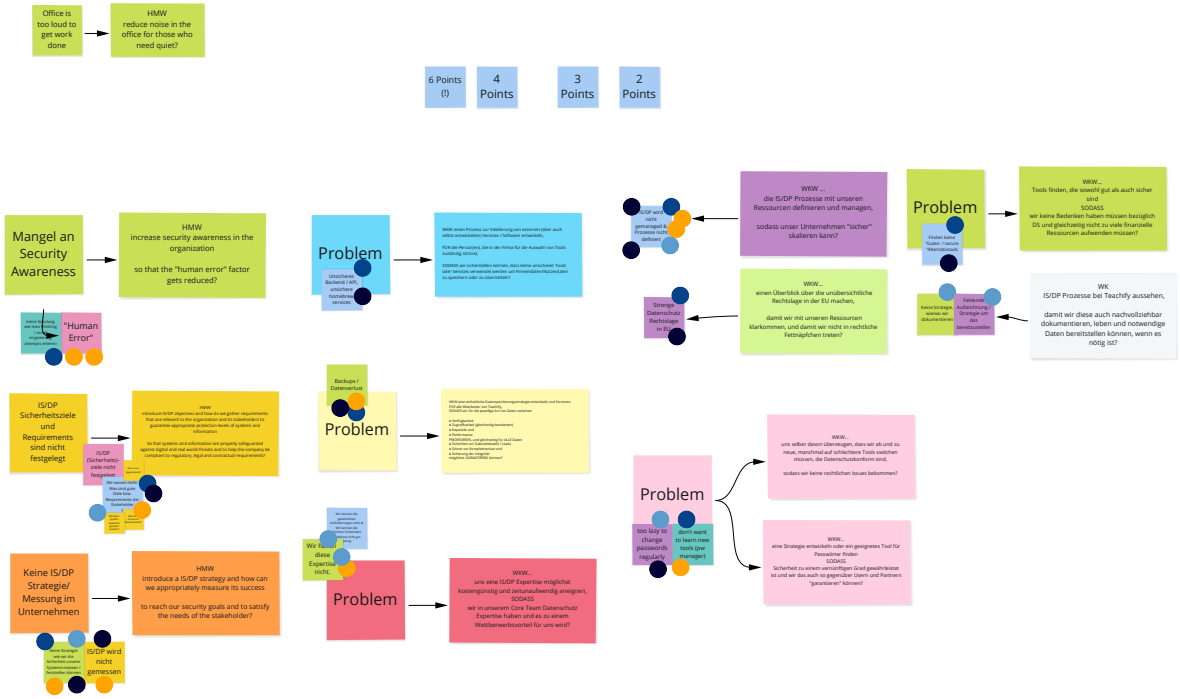


Figure 9.8.: How-Might-We questions to the previously prioritized problems.

a problem, then they had to move on to the next problem and do the same there. Once a participant suggested a solution to each problem, the next cycle of ideation started. These cycles would repeat until the end of a specified time frame. As already mentioned, the selection of *one* solution that will receive an experimental implementation to solve the problem is chosen by another round of Dot Voting. Since there was an individual vote for each problem-solution pair it was possible to ensure that all problems would be addressed in the end. This was done on purpose because filtering out problems was part of a previous task and the ones that were still present at that point would all be required for the final task. During this voting process, four of the problems-solution pairs received an equal vote on some of their proposed solution. This was resolved by discussing each voted for proposed solution to reach consensus and pick only one. In the end, all dots, whether they voted for the ”winner” or not, were grouped together on that solution to have a clearer overview and to make the voted solution easier to find visually.

After the ideating process when all participants looked at the other suggestions, some of them appeared to be rather similar or to have practically the same result if implemented. These ideas were grouped and connected by thin lines, and also seen as one entity during the voting process. While some of the parti-

cipants mentioned that it was hard to find solutions to some of the problems due to the lack of specialist knowledge, they were still able to come up with solutions and by discussing the tied solutions for reaching consensus one just one, they mentioned that such a discussion was useful for their understanding of what these suggested solutions would entail, as there was an input of knowledge for these points.

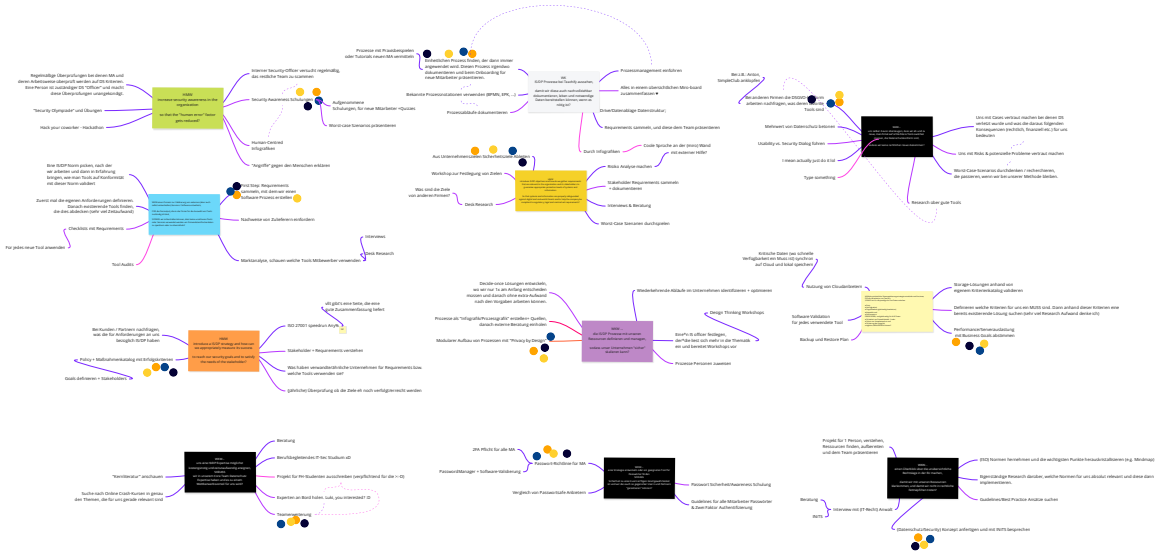


Figure 9.9.: Solution Mind-Mapping for the previously defined most pressing issues.

9.4.4. Commit

The last phase of *The Workshopper Playbook* [107] is the *Commit* phase. In this final phase the previously selected solutions will be prioritized so that an action plan can be created.

During the *Commit* phase the workshop will start off with an *Impact/Effort-Matrix*. Such a matrix is used to map a possible solution/implementation or other task according to its impact and effort [107]. This allows for a quick identification of which solution is the most viable for a possible implementation. A solution that has practically no cost attached but will solve a major problem is an easy win for any organization. A typical approach for assessing the most valuable solution would be top-down and left-right.

The previous task yielded *eleven* solutions that would not have to be assessed and evaluated. This was done by providing each participant with a voting chip. They would place their chip on the matrix according to their own assessment. The center, or focal point of all their individual assessments is what would become the position of the solution on the matrix, which can be seen in figure 9.10. One observation of these assessments is that depending on the degree of (technical) specialist knowledge and background of the participants, some of the assessments were polar opposites. This was used as an opportunity to provide additional information about these points to the participants. In the end, the *ten* most feasible

solutions would be forwarded to the next and final task of the workshop.

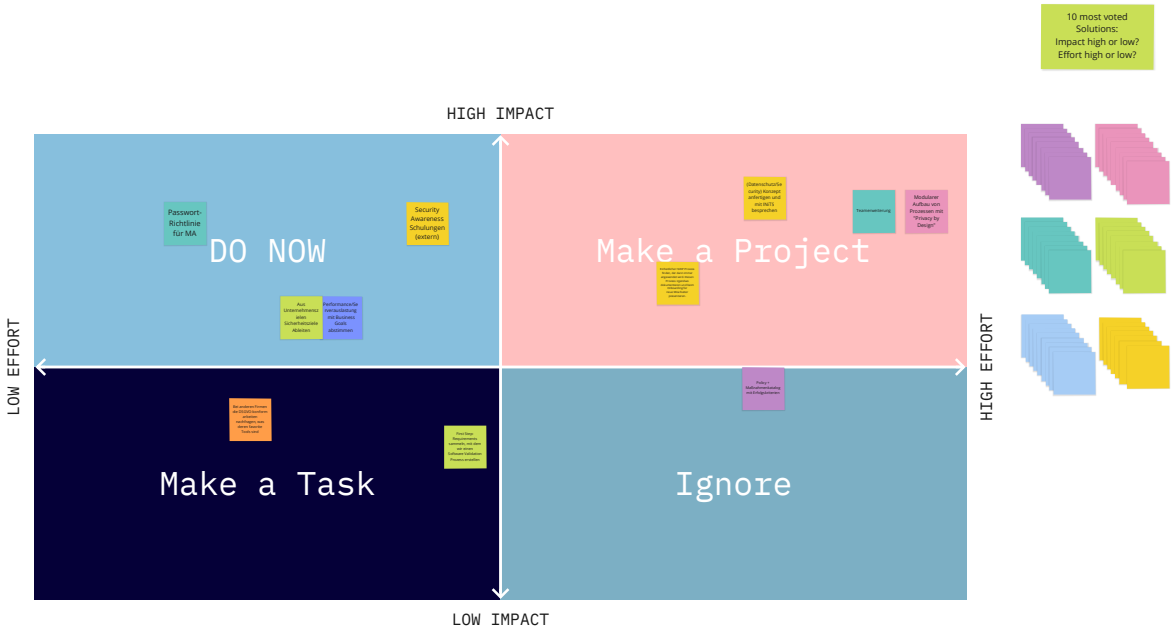


Figure 9.10.: Impact & Effort Matrix of the selected suggested solutions for the most pressing information security and data protection issues.

The final step begins once all solutions have been added to the matrix. According to their positioning based on the previously mentioned relation of impact and effort, these solutions can be prioritized and collected into one action plan [107]. The action plan itself will contain the solution in short, the ”solution experiment”, which is the actions taken as part of the solution to solve the problem at hand, and success criteria for each action. This success criteria can be used at a later stage to evaluate any implemented solution and to assess whether it was successful or another iteration is needed with a new solution. Additionally, each experiment needs to be assigned to a person.

The following figure (9.11) shows the result of this last workshop task. As a starter, the whole group developed a whole ”action” for the first proposed solution. This should help all participants to get a better feeling of how an action can look like and how to define one. After that, the remaining solutions were assigned amongst the participants. Each of them had to specify their assigned actions. Once all actions were defined, they were given a short review and suggestions for improvements for clarity or precision.

As was mentioned by the participants, the prioritization of the tasks according to the Impact & Effort Matrix would make more sense for them at the moment, if low impact-low effort tasks get a higher priority than high effort-high impact tasks, as these ”make a project”-task efforts do surpass the capacity

of the individually assigned persons at the moment. The participants stated that it would be beneficial for them if these high effort tasks would receive their own workshops each.

The creation of such an action plan was welcomed by the participants of the workshop. According to their remarks they went into the workshop without any prior knowledge on the subject and were therefore a bit sceptical of useful results at first, but having a real plan and direction to work towards as a result paired with information provided during the various stages of the workshop gave them confidence that they will be able to actually implement the selected experimental solutions.

Figure 9.11.: The final result of the workshop, an Action Plan for the implementation and verification of the proposed solutions.

10. Evaluation and Discussion

In this chapter the previous research, the SecDT-Framework, and especially the experiment will be evaluated and discussed. Gathered impressions during the workshop and the subsequent interview provided valuable insights for this process. All aspects of this evaluation and discussion can be roughly grouped into the categories *Combination of creative and rigid systems, SecDT-Framework*, and the *Workshop*.

10.1. Combination of creative and rigid systems

While the worlds of Design Thinking and IS/DP seem to be quite contrary at first with one being focused on emotions and creativity, and the other one following relatively strict rules, standards and laws, it was still possible to detect a number of similarities between them.
First and foremost is the focus on humans. In Design Thinking that comes to no surprise, as it is usually something that will be designed for humans. Data protection, especially with the respective laws, are too highlighting the importance and rights of the individual, and what must be done to protect them. So the motivation is definitely different, but in the end it comes down to the same result. Similar to that is the focus on humans in information security. The ”human factor” is one of the biggest threats for security efforts in any organization, as already mentioned in this thesis before. So again, it is not exactly the same, but the focus on humans is unmistakably present and depending on the type of organization, it could very well be the most important one. Besides technology and processes, humans are the third important pillar in information security, with the other two being dependant on the actions of humans. So by finding a ”human-centered” approach to these issues, it can prove to be extremely effective, especially in organizations where there is a strong focus on human-centered behaviour and strategies already, as these would synergize the best.
More of these combinations have been described in chapter 8, where there are also some incompatibilities included. If creative methods are to be used as the main way of securing an organization, it is important to find solutions to these incompatibilities. Especially the issue of legal regulation could be a dampener for creative work, as there will be requirements that simply ”have to be implemented”. No amount of creative work can spare the implementation of such requirements. It would however be possible to make

a project for each of these requirements in which a creative approach is used to satisfy them.

10.2. SecDT-Framework

According to the partner organization, the SecDT-Framework worked very well for them. While they knew about the existence of information security and data protection, it has never been part of their concerns so far, as it is not a very graspable topic for people that are not specialized on it. In the end however they stated that they now feel confident enough to tackle the first set of issues and that they now have at least the needed basic understanding of the matter, for the first iteration.

The SecDT-Framework is likely to behave slightly differently based on the background of the participants. For example, if the participants are all security specialists themselves, there won't be a need for introductions to the topic or further literature. It is also very likely that the tools used to determine problems and solutions would vary as well. This is because of technical or organizational depth of an issue that a certain group of participants is simply not able to reach. So while the framework was tested with and approved by *Design Thinkers*, another experiment with security or technical experts could yield additional insights about the effectiveness or applicability of the framework.

The creative Design Thinking approach worked very well for the introduction of the rather complex topic of IS/DP and the partner organization stated that they strongly believe that such a framework works very well for start-ups or smaller companies that do not have the resources for dedicated security expert personnel, as this approach works very well in making such a complicated topic much more accessible. Nonetheless, they also stated that multiple iterations and a continuous usage of the proposed cycle are definitely necessary and desired, so that the organization can gradually improve, solve any prevalent issues, and to ensure ongoing security operations. To add to that, in an interview shortly after the experiment, the COO of the partner organization even stated that cyber security implementations would never have happened in the first place, if it wasn't with the help of Design Thinking. The reason that was given for such an absolute statement is that simply "doing" security is tedious and dry. It also sparked their interest in trying a similar approach for other rigid topics. Additionally, it came to a big surprise how much can be done in a relatively short amount of time (a first complete action plan with terminated and verifiable outcome in just 5 hours).

10.3. Workshop/Experiment

Since none of the workshop participants had a background of information security or data protection, their impressions, statements, results, and feedback are very likely to be influenced by that fact. As it

would be if all participants were information security experts but had no knowledge about Design Thinking or its processes and tools. They are however familiar with Design Thinking, as they are using some of its tools on a daily basis.
Due to their lack of knowledge on the specific topics they also stated that such a workshop would probably not work well if none of the participants or workshop enablers are already familiar with the subject to appropriately steer the participants in the right directions and prevent them from stagnating. They did however agree that such a workshop works extremely well if it is held by a consultant or when the participants get a specialist companion with them for subject-specific questions or information.

Before the workshop It was very welcomed by the participants to receive input information, as they would have struggled with the topic of information security and data protection due to the lack of sufficient knowledge on the matter, which they also stated as one of their fears before the workshop as the topic was very unfamiliar to them. However, they felt that the amount of input information could still be increased. This could be done by a keynote speech, with a lightning demo, or by ”homework”, as one of the participants mentioned. This homework was meant in a sense that all participants have to prepare something for an upcoming workshop, which will then be assessed and elaborated on.

During the workshop The participants were asked about how they feel with the current task, their state of knowledge and whether there was something missing for them between each tasks. This was received positively, as it enabled discussions on some aspects, which either deepened their understanding or prevented misunderstandings. Such discussions in-between tasks can also ensure a relaxed atmosphere that breaks with the feel of simply having to follow a rigid plan with no opportunity to address other issues or questions.
To further elaborate on that thought, the participants also mentioned that such a workshop works very well to account for all voices in an organization (or at least all voices of the people involved). Such an approach is inclusive and could reveal problems that might be overlooked otherwise. One of the benefits of such an inclusive approach is that the number of people involved increases drastically, which would also subsequently result in an increase of security awareness, as it no longer is something where there is a person specifically tasked with such issues, but it becomes a central element of all people involved.
One of the very basics of a Design Thinking process proved to be exceptionally appropriate to facilitate the understanding of a problem and which ramifications it can have. By gradually moving on and becoming more and more precise in a problem-solution process, it helped the participants to fully grasp what and why something is actually a problem. Additionally, this progressive advance also helped with not being flooded with information at once, as each tasks and stage could be discussed individually.

After the workshop One of the participants mentioned that he was not expecting an actual plan or concrete instructions as a result of the workshop, rather just a general idea of what would be good or bad or simply to use some Design Thinking tools. He highlighted the importance of such results and that a structured and prioritized list of tasks, the *Action Plan*, is of immense value not only for them to know what and when it should be done, but also to have something similar to a guideline to work with. Furthermore, the specification of a time frame for the completion of a task was welcomed by the participants. With a set deadline it becomes palpable and conceivable as opposed to just having a general direction to work with and no set time for a completion.

Similar to how well received information input was at the beginning, the participants stated that it would be beneficial to be provided with additional literature or guiding directions after the workshop to help them consolidating their knowledge even further and to ensure that the actions specified in the Action Plan can be carried out adequately. It would also help them to avoid pitfalls and false information that could become a problem when such an information gathering is done without guidance. This is definitely a good approach and should be included in future workshops or alternatively, a knowledge base with detailed information could be made accessible. However, this problem should not occur when the participants themselves are experts on information security or data protection already.

Likewise the participants stated that the *Impact & Effort Matrix* is a great tool, but they would rather prioritize the low-effort-low-impact tasks over the high-effort-high-impact tasks, as these should result in a new project, which in turn would require an entire workshop for each of these issues to get to the core of them. This too is likely not that much of an issue for persons that are well aware and familiar with most of the topics already. Feedback was also given about the voting system of focal points to determine the actual position on the matrix which was used in the experiment. It serves as a further opportunity to hear and include all voices and to discuss uncertainties or doubts.

All in all, the workshop was received very well and at the end the participants had no doubt left that such a workshop would greatly benefit them in their ability to tackle security issues. It is even possible with limited knowledge on the matter, because by simply turning it into a group effort there are many points of view that will be considered, which can shed a light where there would be none otherwise.

11. Conclusion

In this thesis, the importance of the ”human factor” for information security was highlighted, as well as the severe lack of empathy and regard for the actual humans behind it. Although they make up a major part of all flaws and breaches, and have been repeatedly identified as the weakest link in any cyber security program, there has been little focus on *securing the human*, except for the usual awareness programs or training. Seldom is there any approach that tries to understand the problems at hand and why humans act the way they do in a security environment. The approach chosen for this task was to combine Design Thinking with the world of cyber security. Design Thinking as it is has a strong focus on the individual and tries to fully grasp what the actual problem is, so it can provide a fitting solution that is tailored to the affected person. By doing that, this new school of thought on cyber security elevates the individual so that it becomes the centerpiece of all security efforts.

To achieve this overall goal it was important to first analyse the fundamentals of the worlds of Design Thinking, Information Security and Data Protection. When looking at these three fields completely generically, one of their similarities is that they all have a set of objectives, principles, methods and tools. That alone is however nowhere near enough to validate a combination, as it’s simply not possible to just tie these together. At first, it was assessed that in principle, all different (process) models used in Design Thinking basically follow the exact same pattern. There are always stages about a problem, followed by stages about a solution. The only part that changes are the different tools that can be used during each stage. This insight would be essential during a later phase of this thesis. The other half of this work, the stiff world of standardisation and regulation of information security and data protection is built a bit differently. Although there too are problems that have to be solved, the entire process of solving a problem is not focused on creativity, but rather on risk assessments, strict plans, and simply assigned tasks and deadlines where the individual is only considered after the fact when they have to follow new rules.

Nonetheless, after assessing these completely different worlds, a number of similarities could be identified. Continuity and continual improvement are important factors for all. While it is more obvious with structured systems like an *Information Security Management System* where continual improvement is part of the regulation, it is equally as important in Design Thinking. Especially considering methods like a *Design Sprint*, which is virtually built on the idea of iterative and continuous work. Other similarities

would be the availability of resources, which is vital for all other operations to function properly, and that all sides agree on the importance of the individual/employee or customer, albeit the motives are slightly different. The most difficult obstacle to overcome is however dealing with standardization and regulatory requirements. There is no creative way for defining these. Especially legal requirements must be taken for what they are. Regardless of that, it is still possible to simply take such requirements as the *problem statement* of a new Design Thinking process.

The chief task of this thesis was therefore the creation of an experimental framework (9) which accounts for the lack of empathy and trust in traditional cyber security environments. The SecDT-Framework (Security Design Thinking Framework) tries to offer a new way of introducing complex topics like information security or data protection. It uses the managerial approach for a controlled and managed system that is enhanced with the creativity and flexibility of Design Thinking. By combining "the best of both worlds" it offers a structured and measurable approach for organizations, while it grants the affected individuals working on it the freedoms needed for creative problem-solving. This problem-solving for cyber security issues was tested in an experiment with a partner organization. In this experiment (9.4), we used Design Thinking tools to identify, assess and prioritize cyber security issues and threats, which resulted in a first action plan of immediate measures and safeguards to be implemented.

While at first it seemed virtually impossible to combine the creative world of Design Thinking with the rigid and strict worlds of Information Security and Data Protection with all their regulations, standards and laws, a way was found to incorporate central elements of both and to compound it into one cohesive framework. A number of inferences have been drawn in the chapter *Evaluation and Discussion* (10) already, where it was also discussed which parts of the experimental framework bring benefits and where there is still room for improvement. The experiment and the subsequent interview affirmed that the SecDT-Framework is well received and motivates an organization that had previously barely any association with cyber security to implement safeguards and measures, and to continuously improve their levels of security. Nonetheless, the fact that such a serious topic could be approached in a creative way that is only made possible by using Design Thinking and it still resulted in a proper action plan of measures and safeguards was perceived as an extremely important outcome. According to the current research results it can therefore be assessed that the SecDT-Framework would work best in an environment where creative and agile work methods are already in use, preferably Design Thinking in particular, and where there is at least one security professional for the provision of knowledge and guidance during the implementation and for the operation available, or the resources to consult an external expert.

One of the results of the experiment was that even though the framework itself was well received and welcomed by the partner organization, it would be extremely difficult for them to keep it operating on

their own without an expert as either a consultant or an internal specialist to operate it. Furthermore, the framework has only been tested with a rather small organization where cyber security had not been in the focus before. Assessing the viability of the SecDT-Framework with a larger organizations where there are security experts already and where security processes have been determined before could yield different results. Another limitation is that especially for smaller organizations without any knowledge about cyber security, they would still need an expert to properly operate the framework.

In conclusion, while the SecDT-Framework is considered a success overall, there are still opportunities for improvement. First and foremost, a multitude of experimental runs with organizations of various sizes and fields would be useful to assess the optimal form of an organization that is the most compatible with this framework. Another opportunity would be to formalize the entire framework by creating complete toolboxes and templates so it can work as an ”off-the-shelf” product, which would make it a lot more accessible. Additionally, the provision and sharing of relevant (cyber security) information and knowledge could be improved on, as this proved to be one of the major concerns for an organization with no previous knowledge on the matter.

A. Interview

A final interview with one of the partners as part of the retrospective of the collaboration event was conducted to allow a better assessment and evaluation of the framework. Interviews as a method have been described already (4.6). The interview itself was held in German, so the following is a translation of the transcribed original version. The interviewed person was the COO of the partner organization.

Q1: What is your assessment of the state of information security and data protection in your organization before applying this framework?

We knew that it is an important thing because we've come across GDPR and data protection issues before. However, the awareness of IS/DP was not really high, and very simple things, such as a password manager or 2FA were not implemented yet. It also made us more aware of human errors too.

Q2: Do you think the overall state of security in your organization has improved after the first iteration cycle of the framework? If so, what would you say was the most important improvement or the biggest benefit?

I would say yes with a small no. We haven't implemented the "Do-Now-Tasks", nor the "Make a task" or "Make a project" yet, however, we now have an action plan on how to move on. We know which components we should consider in the future and the workshop definitely raised our awareness about IS/DP, and made the potential problems more understandable.

Q3: What do you think is the greatest benefit of using this framework as compared to the traditional approach?

The methods are visually pleasing and feel more "human-centered". The two workshops were rather interactive brainstorming than lectures, traditional corporate training, and boring consultations. Everyone gets to say/write their opinion. However, it is very important to have someone, who has actual expertise in the field of IS/DP, to run this kind of workshop. Or at least to have someone else in the workshop.

Q4: Would you have thought about introducing information security to the organization without using Design Thinking or creative methods?

No, never. It is such a tedious and dry subject. I wouldn't know, how to combine creative thinking with something that non-creative. Maybe I should give it a try to introduce other tedious topics to the team

with design thinking methods!

Q5: Was there any point during the Workshop where you felt lost or out of place? If so, why?

Yes, sometimes I had the feeling, that we don't know whether we've covered every aspect of IS/DP. In those times it was great that we were able to ask you questions. However, I'd like to have more literature or guidance for the action plan (especially for the "make-a-project" tasks). I know how to start each task, but the fear that we might have missed an important aspect is lingering at the back of my head.

Q6: What was your highlight of the Workshop and why?

Although we almost knew nothing about IS/DP before the workshop, 1) we now have an idea of information security, 2) we now have discussed the most pressing issues, and 3) we now have a reasonable action plan to start implementing everything and the best thing is that we did it in such a short time!! It was only 5 hours!

Q7: Do you think that there is a missing element in the SecDT-Framework, or is there something that should be added to improve the system?

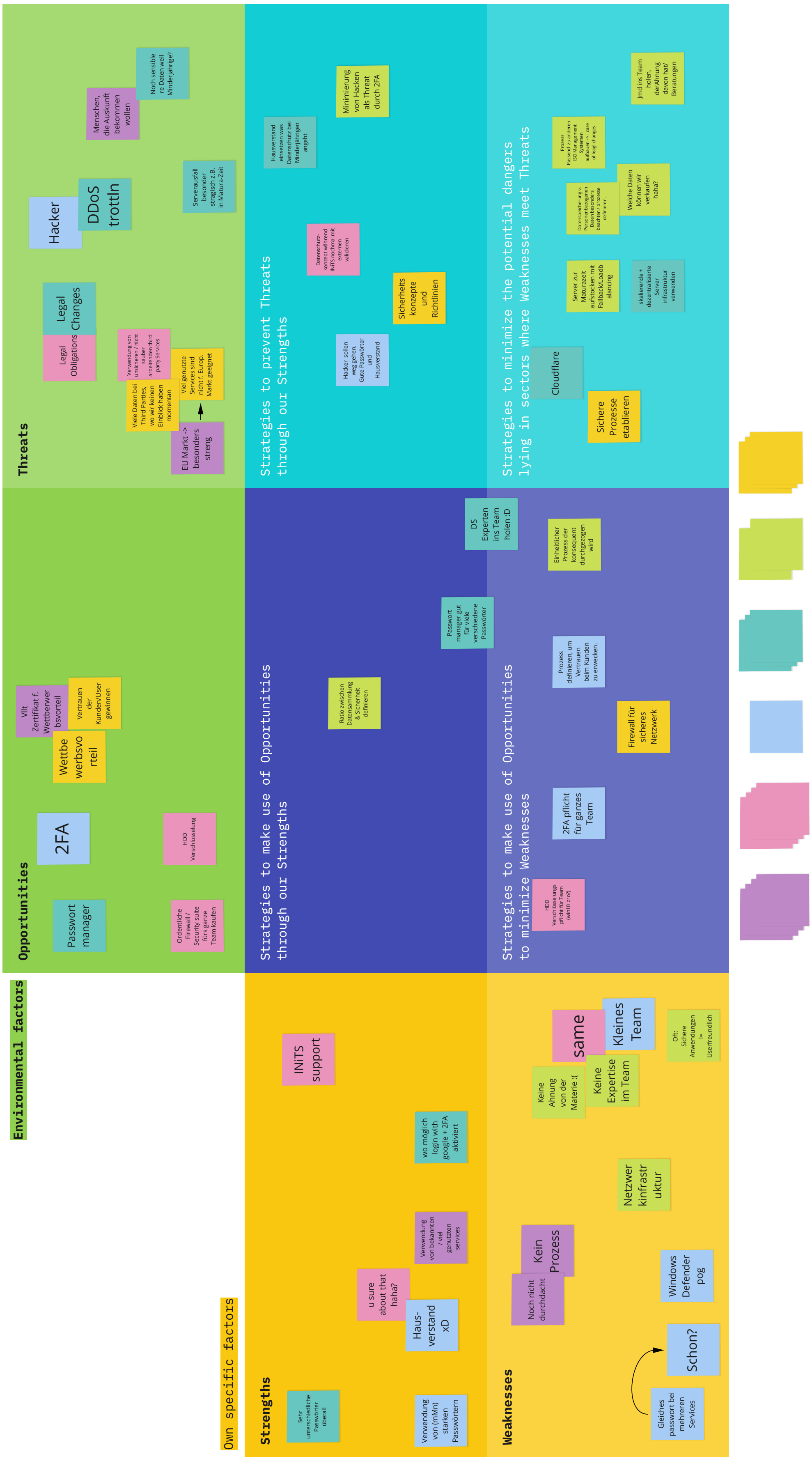
This depends. This kind of SecDT-Framework works great with guidance of a professional in this field, who understands IS/DP and DT. However, most start-ups don't have the expertise on the team, and don't have the money to get this expertise. Therefore, it might be helpful to have methods or stages with actual research in it (e.g. do desk research, or read the norm, or use lightning demos). Another solution would be a verification phase by experts, e.g.: go and implement something, then do an interview with experts!

Q8: Would you recommend the SecDT-Framework to other organizations? If yes, why and to which types of organizations would you recommend it?

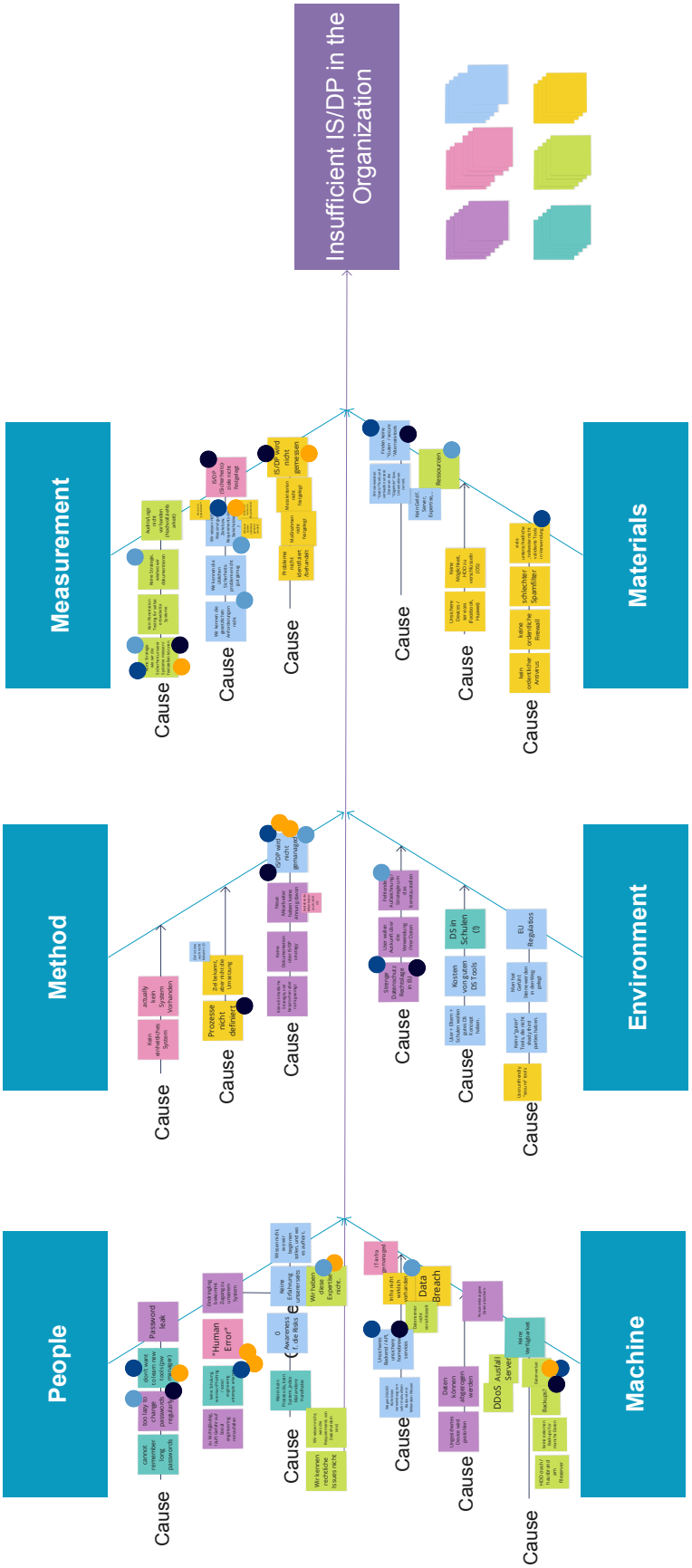
I would love to recommend Design Thinking to any kind of company. However, at this stage, the framework itself might be difficult to be implemented by start-ups, because they probably don't have information security experts on the team (and I suppose some don't know how to run design thinking workshops either). Nonetheless, I would definitely recommend the service of you (someone who knows about IS/DP and DT) in combination with the SecDT-Framework. I would also recommend larger companies to try out this framework! Usually they have the money to get an IS/DP expert onto the team. That person should familiarize him-/herself with design thinking and try out this framework. Especially in larger companies, there are so many different departments with so many different security issues. It would be great to hear their voices, understand their point of view and get their opinions. However, most meetings in such large companies are so long and boring, because mostly, only two people are arguing about irrelevant stuff, resulting in more confusion. Therefore, it would be great to try out the SecDT-Framework to get and share everyone's opinion within a reasonable timeframe.

B. Workshop Results

This annex contains higher resolution figures of the workshop ”whiteboards”.


Environmental factors
Threats
Opportunities
Own specific factors
Strengths
Weaknesses
Strategies to prevent Threats through our Strengths
Strategies to minimize the potential dangers lying in sectors where Weaknesses meet Threats
Strategies to make use of Opportunities through our Strengths
Strategies to make use of Opportunities to minimize Weaknesses
Hacker
DDoS trottln
Legal Changes
Legal Obligations
EU Markt -> besonders streng
Passwort manager
2FA
Wettbewerbsvorteil
Minimierung von Hacken als Threat durch 2FA
Sicherheits konzepte und Richtlinien
Cloudflare
Sichere Prozesse etablieren
2FA pflicht für ganzes Team
Firewall für sicheres Netzwerk
INITS support
Haus-verstand xD
u sure about that haha?
Kein Prozess
Noch nicht durchdacht
Windows Defender pog
Schon?
Netzwerkinfrastruktur
same
Kleines Team
Keine Expertise im Team
Keine Ahnung von der Materie :(


Marketing
facebook
TikTok
Youtube
Social Media plattformen
Ad networks
AMS (?)
WKO
DS einheitlich geregelt innerhalb EU, oder?
EU Gesetze (?)
Österreich (Gesetze)
Datensc hutzbeh örde
Finanzamt
Bildungs-ministerium
Advisory Board
Consulting
NGOs?
App stores
XR Frameworks
Backend (e.g. aws)
Eltern
Geschwister
Technische Services f. Entwicklung
Frontend (e.g. flutter, unity)
Webhoster
Lehrer
Smartphone Hersteller
Website CMS
Investoren
Schüler
User
Open Source Code Services
Unternehmen
Schule
Business partner
(Lehramt) Studenten
Direktionen
Angehende Lehrlinge
Universitäten
KMUs
Lieferanten?
Andere Startups im EdTech bereich
Forschu ngseinric htungen
HR
Austauschpla ttformen
eTwinning
Management
CRM
Third party services
Externe comm tools (zB Mail, Mailchimp)
Mitarbeiter
Designer
IT-Abteilung?
WhatsApp
Comm tools
Discord
Programmierer
Firmen-interne comm tools (discord)
Miro
Gründer Team
Brilliant Lol
Google Drive, Gmail, Google Calendar
Productivity tools
Headspace Lol
Clockify
ClickUp


Insufficient IS/DP in the Organization
Measurement
Materials
Method
Environment
People
Machine
Cause
Password leak
*Human Error
Data Breach
DDoS Ausfall Server

Move Stakeholders to the Map

Understand how each stakeholder can help the team, how involved they should be and who to contact when things come up.

Core Team

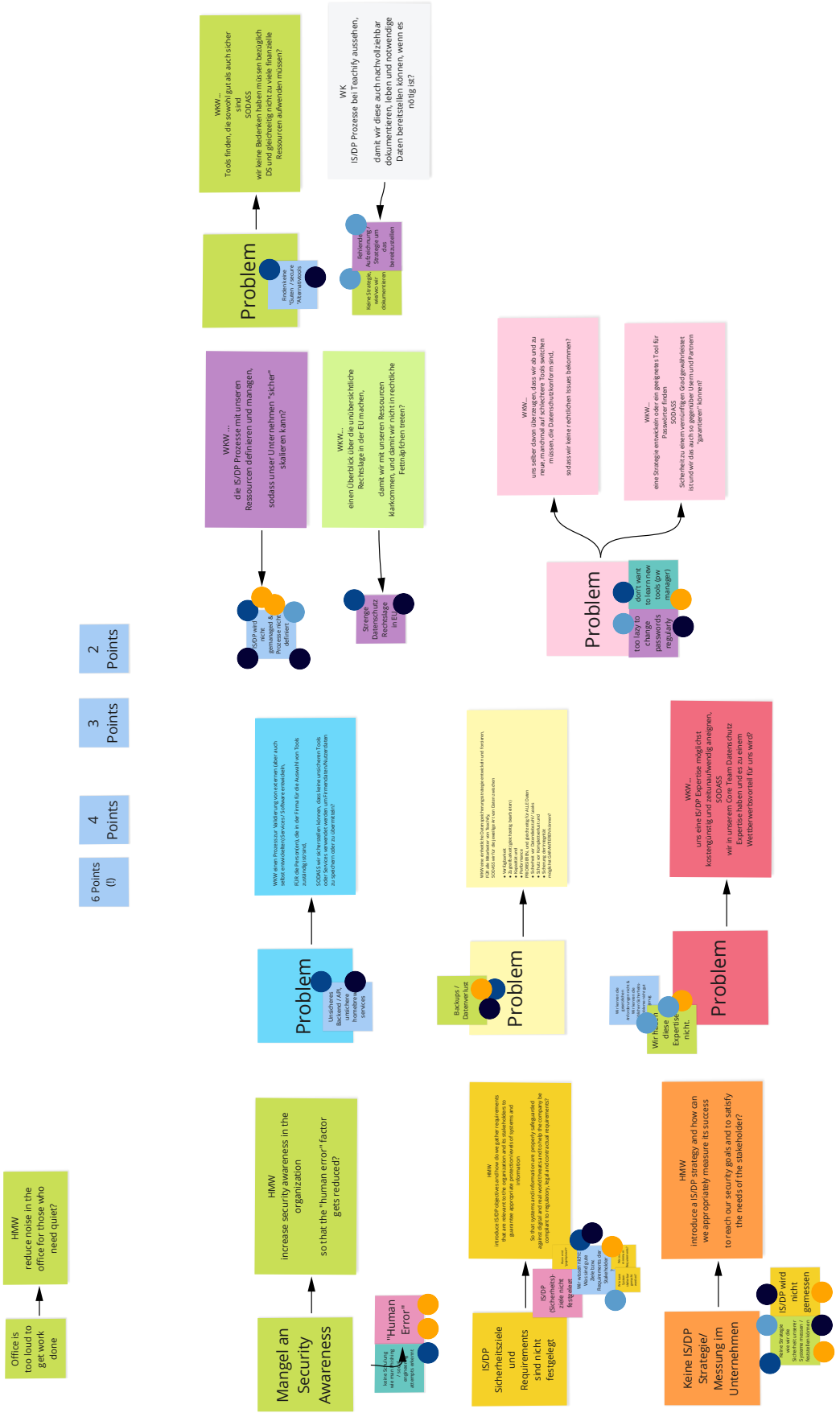
Full time on the project/team (e.g., PMs, engineers, designers)

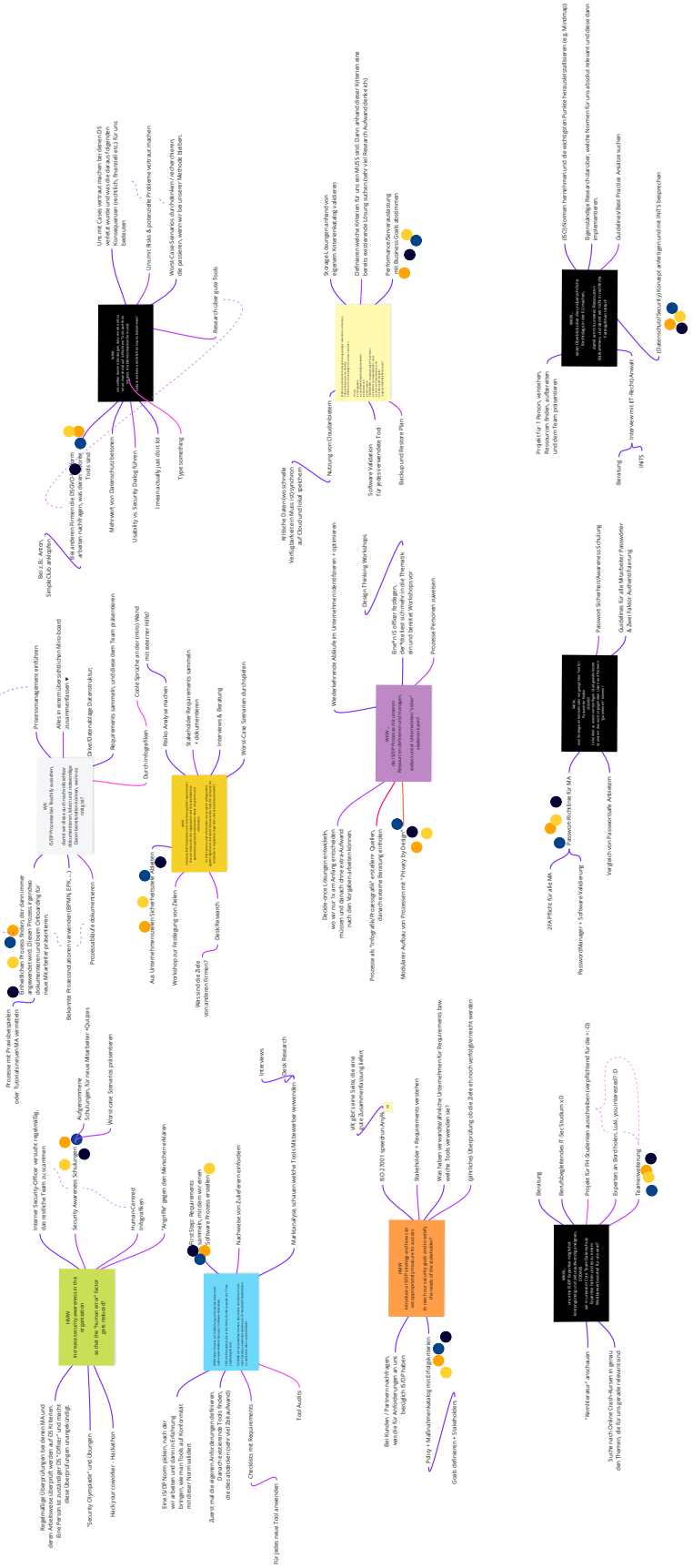
Involved

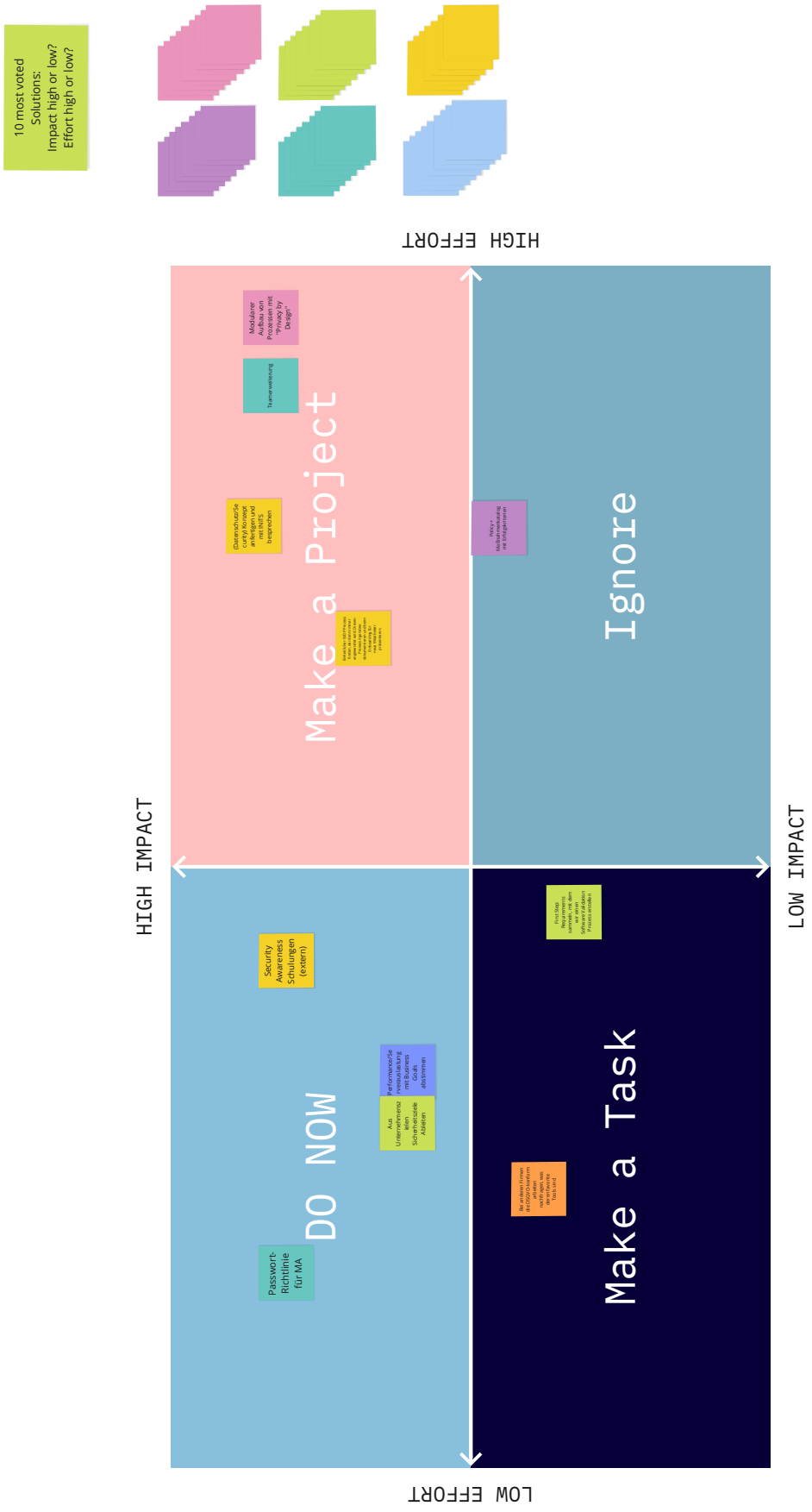
Regularly providing input or helping to move work forward, but this project is not their sole focus

Informed

Wants to stay up to date and will provide feedback/input when necessary


HMW reduce noise in the office for those who need quiet?
Office is too loud to get work done
HMW increase security awareness in the organization so that the "human error" factor gets reduced?
Mangel an Security Awareness
"Human Error"
HMW introduce ISMS objectives and drive gather requirements that are relevant to the organization and its stakeholders to guarantee appropriate protection of systems and information
ISMS (Sicherheits)-ziele nicht festgelegt
ISMS Sicherheitsziele und Requirements sind nicht festgelegt
HMW introduce a ISMS strategy and how can we appropriately measure its success to reach our security goals and to satisfy the needs of the stakeholder?
Keine Strategie, Aufzeichnung / Messungen um diese zu dokumentieren
Keine ISMS Strategie/ Messung im Unternehmen
ISMS wird nicht gemessen
Problem
Unsichere Backend / API, unsichere homebrew services
Backups / Datenverlust
Problem
Problem
Problem
Problem
too lazy to change passwords regularly
don't want to learn new tools (pw manager)
Wir haben diese Expertise nicht.
Problem
Problem
WKW... Tools finden, die sowohl gut als auch sicher sind SODASS wir keine Bedenken haben müssen bezüglich DS und gleichzeitig nicht zu viele finanzielle Ressourcen aufwenden müssen?
WK ISMS Prozesse bei Teachify aussehen, damit wir diese auch nachvollziehbar dokumentieren, leben und notwendige Daten bereitstellen können, wenn es nötig ist?
WKW... die ISMS Prozesse mit unseren Ressourcen definieren und managen, sodass unser Unternehmen "sicher" skalieren kann?
WKW... einen Überblick über die unübersichtliche Rechtslage in der EU machen, damit wir mit unseren Ressourcen klarkommen, und damit wir nicht in rechtliche Fettnäpfchen treten?
WKW... uns selber davon überzeugen, dass wir als und zu mehr, mindestens auf ISO-Niveau, sichern müssen, die Datenschutzkonform sind, sodass wir keine rechtlichen Issues bekommen?
WKW... eine Strategie entwickeln, der geeignetes Tool für Passwörter finden SODASS Sicherheit zu einem vernünftigen Grad gewährleistet ist und wir das auch so gegenüber Kunden und Partnern garantieren können?
WKW... uns eine ISMS Expertise möglichst kostengünstig und zeitunaufwendig aneignen, SODASS wir in unserem Core Team Datenschutz Expertise haben und es zu einem Wettbewerbsvorteil für uns wird?
2 Points
3 Points
4 Points
6 Points (!)




10 most voted Solutions: Impact high or low? Effort high or low?
HIGH EFFORT
LOW EFFORT
HIGH IMPACT
LOW IMPACT
Make a Project
Ignore
DO NOW
Make a Task
Security Awareness Schulungen (extern)
Passwort-Richtlinie für MA


#1
Passwort-Richtlinie für MA
DO NOW
31.07.
Solution Experiment:
- Rausfinden was ein gutes Passwort ausmacht
- Wo sollten welche Passwörter oder Passwortanforderungen notwendig sein?
- Passwortmanager suchen
- Richtlinie schreiben und Dokument für alle MA zugänglich ablegen
- Checkliste
- Nicht im Browser abspeichern
2 Wochen nach Implementierung, alle nachfragen, ob Checkliste erfüllt wurde.
#2
Security Awareness Schulungen (extern)
DO NOW
31.07.
Solution Experiment:
- Mehrere ext. Schulungen präsentieren
- Pro und Contra abwägen, alles dokumentieren und präsentieren
- Abstimmung über beste Lösung
- Kontaktaufnahme mit jeweiligen Firmen
Success Criteria: Informierte Entscheidung ob, wann und wie wir
Vielleicht Kriterien ab wann eine Schulung notwendig ist?
#3
Aus Unternehmenszielen Sicherheitsziele Ableiten
DO NOW
31.07.
Solution Experiment:
- Klar definierte Unternehmensziele ausarbeiten
- Research bezüglich Requirements Sicherheit von vergleichbaren Unternehmen
- Ziele ableiten, dokumentieren und präsentieren
Success Criteria: Klar definierte Sicherheitsziele die mit unserem BM konform sind. Anforderungen für Services sind definiert
#4
Performance/Serverauslastung mit Business Goals abstimmen
DO NOW
31.7.
Solution Experiment:
- Business goals dahingehend analysieren, wofür Daten gespeichert und verarbeitet werden müssen
- Kriterienliste erstellen nach denen Datenspeicher bewertet wird (Performance, Sicherheit, Kosten, ...)
- Liste von möglichen Speicherformen erstellen und nach Kriterienliste bewerten
- Für jeden Daten speichernden business prozess kriterien anwenden und passende speicherformen finden.
Success Criteria: Für jeden Datenverarbeitenden Prozess mögliche Speicherform vorschlagen, die den Anforderungen gerecht wird.
Success Criteria: Anpassung der Business goals, sodass Anforderungen an Datenspeicher als Zielhardcoded sind
#5
(Datenschutz/Security) Konzept anfertigen und mit INITS besprechen
MAKE A PROJECT
Im Rahmen v. Inits
Solution Experiment:
- Requirements sammeln
- Security Schulung/ Desk Research berücksichtigen
- Grobkonzept erstellen
- Abstimmen mit Business Goals & Security Goals (#3 & #4)
- mit Inits Besprechen
- Anpassen
-mit IT-Rechtsanwälten besprechen
Success Criteria: Konzepts, das von inits Rechtsanwälten besprochen wurde und für gut empfunen wurde.
#6
Gamerweiterung
MAKE A PROJECT
Im Rahmen v. Inits
Solution Experiment:
- Klare Definition der Rolle, Funktion, Aufgaben, Anforderungen und Bezahlung für die Person
- Abstimmung über Notwendigkeit von Teamerweiterung
- Ausschreibung auf LinkedIn? sonst. Job Portalen
Success Criteria: passende Bewerber gefunden; Entscheidung über Erweiterung liegt dann bei uns
#7
Modularer Aufbau von Prozessen mit "Privacy by Design"
MAKE A PROJECT
Im Rahmen v. Inits
Solution Experiment:
- Einarbeiten in Prozessdesign
- Einarbeiten in Privacy by Design
-Erstellung von erstem Entwurf eines Prozessdiagramms
-Validierung mit INITS Experten o.ä. (siehe #5)
Success Criteria: Von Experten validiertes Prozessdesign, das Privacy by Design garantiert
#8
Einheitlicher ISDP Prozess finden, der dann immer angewendet wird. Diesen Prozess irgendwo dokumentieren und neuem Onboarding für neue Mitarbeiter präsentieren.
MAKE A PROJECT
Im Rahmen v. Inits
Solution Experiment:
-Requirements sammeln
- Best Practices suchen & finden
- Prozessdokumentationsart finden
- Mit #5 abgleichen
- Dokumentieren
- Schulung/ Onboarding Slides erstellen
Success Criteria: Prozessplan wurde generiert und dokumentiert, Onboarding Slides dafür sind vorhanden
#9
Bei anderen Firmen die DSGVO-konform arbeiten nachfragen, was deren favorite Tools sind
MAKE A TASK
31.8.
Solution Experiment:
- Firmen/Startups raussuchen, anschreiben
- Ergebnisse dokumentieren
- Ergebnisse präsentieren
Success Criteria: Liste von Tools, mit den entsprechenden Funktionen, die wir auf unseren Case prüfen können
#10
First Step: Requirements sammeln, mit dem wir einen Software Validation Prozess erstellen
MAKE A TASK
31.8.
Solution Experiment:
- Liste von Anforderungen bezüglich Sicherheit und Datenschutz erstellen
- Bewerten wie sich die Anforderungen unterscheiden für interne tools, tools mit Kundendaten, tools mit vertraulichen Firmendaten etc.
-Zum test der Anforderungen die Liste auf alle Tools die aktuell in Verwendung sind anwenden.
Success Criteria: Verwendete Tools sind konform den Anforderungen

List of Figures

Bibliography

[1] Bundeskriminalamt, "Lagebericht Cybercrime 2018 - Entwicklungen, Phänomene und Schwerpunkte," Bundeskriminalamt, Tech. Rep., 2019.

[2] L. Hadlington, "The "human factor" in cybersecurity: Exploring the accidental insider," in *Psychological and behavioral examinations in cyber security*. IGI Global, 2018, pp. 46–63.

[3] A. Ruzicka and A. Niederbacher, "Deloitte Cyber Security Report Österreich 2020 - Eine Studie von Deloitte Österreich in Kooperation mit SORA," Deloitte Österreich, Tech. Rep., 2020.

[4] L. Hadlington, "Human factors in cybersecurity; examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours," *Heliyon*, vol. 3, no. 7, p. e00346, 2017.

[5] R. W. Proctor and J. Chen, "The role of human factors/ergonomics in the science of security: decision making and action selection in cyberspace," *Human factors*, vol. 57, no. 5, pp. 721–727, 2015.

[6] S. R. Team, "Sophos 2020 Threat Report," Sophos, Tech. Rep., 2020.

[7] D. Henshel, M. Cains, B. Hoffman, and T. Kelley, "Trust as a human factor in holistic cyber security risk assessment," *Procedia Manufacturing*, vol. 3, pp. 1117–1124, 2015.

[8] A. Oltramari, D. S. Henshel, M. Cains, and B. Hoffman, "Towards a Human Factors Ontology for Cyber Security." in *Stids*, 2015, pp. 26–33.

[9] C. Meinel and J. Von Thienen, "Design Thinking," *Informatik-Spektrum*, vol. 39, no. 4, pp. 310–314, 2016.

[10] W. Brenner, F. Uebernickel, and T. Abrell, "Design thinking as mindset, process, and toolbox," in *Design thinking for innovation*. Springer, 2016, pp. 3–21.

[11] D. R. Schallmo *et al.*, *Design Thinking erfolgreich anwenden*. Springer, 2017.

[12] B. R. Ingle, *Design thinking for entrepreneurs and small businesses: Putting the power of design to work*. Apress, 2013.

[13] W. Brenner and F. Uebernickel, "Design thinking for innovation," *Research and Practice*, 2016.

[14] A. P. W. McCarthy, "Design Thinking," *Wirtschaftsinformatik & Management*, vol. 9, no. 1, pp. 84–92, 2017.

[15] D. R. Schallmo, *Jetzt Design Thinking Anwenden*. Springer, 2018.

[16] S. Adikari, C. McDonald, and J. Campbell, "Reframed contexts: design thinking for agile user experience design," in *International Conference of Design, User Experience, and Usability*. Springer, 2013, pp. 3–12.

[17] N. M. C. Valentim, W. Silva, and T. Conte, "The students' perspectives on applying design thinking for the design of mobile applications," in *2017 IEEE/ACM 39th International Conference on Software Engineering: Software Engineering Education and Training Track (ICSE-SEET)*. IEEE, 2017, pp. 77–86.

[18] P. Lucena, A. Braz, A. Chicoria, and L. Tizzei, "Ibm design thinking software development framework," in *Brazilian Workshop on Agile Methods*. Springer, 2016, pp. 98–109.

[19] M. Palacin-Silva, J. Khakurel, A. Happonen, T. Hynninen, and J. Porras, "Infusing design thinking into a software engineering capstone course," in *2017 IEEE 30th Conference on Software Engineering Education and Training (CSEE&T)*. IEEE, 2017, pp. 212–221.

[20] M. B. Jensen, F. Lozano, and M. Steinert, "The origins of design thinking and the relevance in software innovations," in *International Conference on Product-Focused Software Process Improvement*. Springer, 2016, pp. 675–678.

[21] J. Schneider and M. Stickdorn, *This is service design thinking: basics, tools, cases*. Wiley, 2011.

[22] P. Pauwels, R. De Meyer, and J. Van Campenhout, "Design thinking support: information systems versus reasoning," *Design Issues*, vol. 29, no. 2, pp. 42–59, 2013.

[23] H. Plattner, "d. school Bootcamp Bootleg," 2010.

[24] N. Direkova, "Design Sprint Methods," 2015.

[25] I. LLC., *Design Thinking for Educators Toolkit*. IDEO LLC, 2012.

[26] F. Dobrigkeit, D. de Paula *et al.*, "The best of three worlds-the creation of innodev a software development approach that integrates design thinking, scrum and lean startup," in *DS 87-8 Proceedings of the 21st International Conference on Engineering Design (ICED 17) Vol 8: Human Behaviour in Design, Vancouver, Canada, 21-25.08. 2017*, 2017, pp. 319–328.

[27] T. Björklund, P. Hannukainen, and T. Manninen, "Measuring the impact of design, service design and design thinking in organizations on different maturity levels," in *ServDes2018-Service Design Proof of Concept*, 06 2018.

[28] L. Kimbell, "Rethinking design thinking: Part i," *Design and Culture*, vol. 3, no. 3, pp. 285–306, 2011.

[29] ——, "Rethinking design thinking: Part ii," *Design and Culture*, vol. 4, no. 2, pp. 129–148, 2012.

[30] J. C. Pereira and R. de FSM Russo, "Design thinking integrated in agile software development: A systematic literature review," *Procedia computer science*, vol. 138, pp. 775–782, 2018.

[31] C. Vetterli, W. Brenner, F. Uebernickel, and C. Petrie, "From palaces to yurts: Why requirements engineering needs design thinking," *IEEE Internet Computing*, vol. 17, no. 2, pp. 91–94, 2013.

[32] T. Lindberg, C. Meinel, and R. Wagner, "Design thinking: A fruitful concept for it development?" in *Design thinking*. Springer, 2011, pp. 3–18.

[33] L. Leifer, H. Plattner, and C. Meinel, *Design Thinking Research: Building Innovation Eco-Systems*. Springer Science & Business Media, 2013.

[34] H. Plattner, C. Meinel, and L. Leifer, *Design thinking research: Building innovators*. Springer, 2014.

[35] ——, *Design Thinking Research: Making Design Thinking Foundational*. Springer, 2012.

[36] J. H. Jörg Freiling, *Entrepreneurship - Gründung und Skalierung von Startups*. Springer, 2019.

[37] M. Nieles, K. Dempsey, and V. Y. Pillitteri, "An introduction to information security," *NIST special publication*, vol. 800, p. 12, 2017.

[38] M. Stamp, *Information security: principles and practice*. John Wiley & Sons, 2011.

[39] S. Samonas and D. Coss, "The CIA strikes back: Redefining Confidentiality, Integrity and Availability in Security." *Journal of Information System Security*, vol. 10, no. 3, 2014.

[40] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE transactions on dependable and secure computing*, vol. 1, no. 1, pp. 11–33, 2004.

[41] ISO/IEC, "Information technology – Security techniques – Information security management systems – Requirements," International Organization for Standardization, Geneva, CH, Standard, Oct. 2013.

[42] "The ISO Survey of Management System Standard Certifications – 2017 – Explanatory Note," https://isotc.iso.org/livelink/livelink/fetch/-8853493/8853511/8853520/18808772/00._Executive_summary_2016_Survey.pdf?nodeid=19208898&vernum=-2, accessed: 2021-02-16.

[43] "The ISO Survey of Management System Standard Certifications – 2019 – Explanatory Note," https://isotc.iso.org/livelink/livelink/fetch/-8853493/8853511/8853520/18808772/0._Explanatory_note_and_overview_on_ISO_Survey_2019_results.pdf?nodeid=21413237&vernum=-2, accessed: 2021-02-16.

[44] J. Geismann, C. Gerking, and E. Bodden, "Towards Ensuring Security by Design in Cyber-Physical Systems Engineering Processes," in *Proceedings of the 2018 International Conference on Software and System Process*, ser. ICSSP '18. New York, NY, USA: Association for Computing Machinery, 2018, p. 123–127. [Online]. Available: https://doi.org/10.1145/3202710.3203159

[45] J. McManus, "Security by Design: Teaching Secure Software Design and Development Techniques," *J. Comput. Sci. Coll.*, vol. 33, no. 3, p. 75–82, Jan. 2018.

[46] M. Kreitz, "Security by Design in Software Engineering," *SIGSOFT Softw. Eng. Notes*, vol. 44, no. 3, p. 23, Nov. 2019. [Online]. Available: https://doi.org/10.1145/3356773.3356798

[47] E. Union, "General Data Protection Regulation," 2016.

[48] M. d. C. Freitas and M. Mira da Silva, "GDPR Compliance in SMEs: There is much to be done," *Journal of Information Systems Engineering & Management*, vol. 3, no. 4, p. 30, 2018.

[49] M. Brodin, "A Framework for GDPR Compliance for Small-and Medium-Sized Enterprises," *European Journal for Security Research*, vol. 4, no. 2, pp. 243–264, 2019.

[50] S. S. Shapiro, "Privacy by Design: Moving from Art to Practice," *Commun. ACM*, vol. 53, no. 6, p. 27–29, Jun. 2010. [Online]. Available: https://doi.org/10.1145/1743546.1743559

[51] S. Spiekermann, "The Challenges of Privacy by Design," *Commun. ACM*, vol. 55, no. 7, p. 38–40, Jul. 2012. [Online]. Available: https://doi.org/10.1145/2209249.2209263

[52] A. Pattakou, A. Mavroeidi, V. Diamantopoulou, C. Kalloniatis, and S. Gritzalis, "Towards the Design of Usable Privacy by Design Methodologies," in *2018 IEEE 5th International Workshop on Evolving Security Privacy Requirements Engineering (ESPRE)*, 2018, pp. 1–8.

[53] A. Cavoukian, "Understanding How to Implement Privacy by Design, One Step at a Time," *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 78–82, 2020.

[54] M. Degeling, C. Lentzsch, A. Nolte, T. Herrmann, and K. Loser, "Privacy by Socio-Technical Design: A Collaborative Approach for Privacy Friendly System Design," in *2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC)*, 2016, pp. 502–505.

[55] A. Cavoukian *et al.*, "Privacy by Design: The 7 Foundational Principles," *Information and privacy commissioner of Ontario, Canada*, vol. 5, 2009.

[56] M. Rost and K. Bock, "Privacy by Design und die neuen Schutzziele," *Datenschutz und Datensicherheit-DuD*, vol. 35, no. 1, pp. 30–35, 2011.

[57] M. S. Bargh and S. Choenni, "Towards Applying Design-Thinking for Designing Privacy-Protecting Information Systems," in *2019 First IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*. IEEE, 2019, pp. 196–202.

[58] P. M. Asquith and P. L. Morgan, "Representing a human-centric cyberspace," in *International Conference on Applied Human Factors and Ergonomics*. Springer, 2020, pp. 122–128.

[59] M. Tyworth, N. A. Giacobe, V. F. Mancuso, M. D. McNeese, and D. L. Hall, "A human-in-the-loop approach to understanding situation awareness in cyber defence analysis," *EAI Endorsed Transactions on Security and Safety*, vol. 1, no. 2, 2013.

[60] J. Klein and K. Hossain, "Conceptualising Human-centric Cyber Security in the Arctic in Light of Digitalisation and Climate Change," *Arctic Review*, vol. 11, pp. 1–18, 2020.

[61] A. Nieto and R. Rios, "Cybersecurity profiles based on human-centric IoT devices," *Human-centric Computing and Information Sciences*, vol. 9, no. 1, p. 39, 2019.

[62] S. Kassicieh, V. Lipinski, and A. F. Seazzu, "Human centric cyber security: what are the new trends in data protection?" in *2015 Portland International Conference on Management of Engineering and Technology (PICMET)*. IEEE, 2015, pp. 1321–1338.

[63] "What is Design Thinking and Why is it so Popular?" https://www.interaction-design.org/literature/article/what-is-design-thinking-and-why-is-it-so-popular, accessed: 2021-03-23.

[64] "Customer Journey Management Platform | Touchpoint Dashboard," https://www.touchpointdashboard.com/, accessed: 2021-03-23.

[65] "Miro Online Whiteboard for Visual Collaboration," https://miro.com/, 2021, accessed: 2021-07-02.

[66] "What is Miro?" https://help.miro.com/hc/en-us/articles/360017730533-What-Is-Miro-, 2021, accessed: 2021-07-02.

[67] "Mural Digital Workspace," https://www.mural.co/, 2021, accessed: 2021-08-02.

[68] "MITRE Innovation Toolkit," https://itk.mitre.org/, 2021, accessed: 2021-07-02.

[69] "Design Thinking Activities and Tools - Enterprise Design Thinking," https://www.ibm.com/design/thinking/page/toolkit, 2021, accessed: 2021-08-02.

[70] "Design Kit," https://www.designkit.org/methods, 2021, accessed: 2021-08-02.

[71] "Customer Journeys vs User Journeys: Why it's important to differentiate," https://www.answerdigital.com/retail/customer-journey-vs-user-journey, accessed: 2021-03-24.

[72] S. Poguntke, "Design Sprint," https://wirtschaftslexikon.gabler.de/definition/design-sprint-54275, accessed: 2021-04-29.

[73] "Why is information security needed," https://shop.bsigroup.com/Browse-By-Subject/ICT/Information-security-standards-and-publications/Why-is-information-security-needed/, accessed: 2021-05-17.

[74] "What is Information Security and why it is important," https://blog.eccouncil.org/what-information-security-is-and-why-it-is-important/, accessed: 2021-05-17.

[75] H. Singh, "3 Principles of Information Security | Definition," https://thecyphere.com/blog/principles-information-security/, accessed: 2021-05-17.

[76] M. Burnette, "Three Tenets of Information Security," https://www.lbmc.com/blog/three-tenets-of-information-security/, accessed: 2021-05-17.

[77] "Confidentiality, Integrity, Availability (CIA Triad) - The Backbone of Cybersecurity," https://medium.datadriveninvestor.com/confidentiality-integrity-availability-cia-triad-the-backbone-of-cybersecurity-8df3f0be9b0e, accessed: 2021-06-24.

[78] M. E. Whitman and H. J. Mattord, *Principles of information security*. Cengage Learning, 2011.

[79] "Pillars of Security, People, Organization of Information Security - The InfoSec Handbook," https://ebrary.net/26644/computer_science/pillars_security, accessed: 2021-06-24.

[80] ISO/IEC, "Information technology – Security techniques – Code of practice for information security controls," International Organization for Standardization, Geneva, CH, Standard, Oct. 2013.

[81] B. Von Solms, "Corporate governance and information security," *Computers & Security*, vol. 20, no. 3, pp. 215–218, 2001.

[82] "Governance - Bedeutung im Cambridge English Wörterbuch," https://dictionary.cambridge.org/de/worterbuch/englisch/governance, accessed: 2021-06-24.

[83] "ISO 27001 definition: What is iso 27001?" https://www.itgovernance.co.uk/iso27001, accessed: 2021-06-28.

[84] ISO/IEC, "Quality management systems - Requirements," International Organization for Standardization, Geneva, CH, Standard, Sep. 2015.

[85] S. Ristov, M. Gushev, and M. Kostoska, "Information Security Management System for Cloud Computing," *ICT Innovations 2011, Web Proceedings ISSN 1857*, vol. 7288, p. 49, 2012.

[86] A. Wiedemann, "Risikoappetit - Definition," https://www.gabler-banklexikon.de/definition/risikoappetit-81632, accessed: 2021-06-24.

[87] "Risk appreciation according ISO 31010," https://www.globalsuitesolutions.com/iso-31010-and-risk-appreciation/, accessed: 2021-06-29.

[88] ISO/IEC/ÖVE/ÖNORM, "Risk management – Risk assessment techniques," International Organization for Standardization, ÖNORM, Geneva, CH, Standard, Dec. 2010.

[89] S. Brathwaite, "Types of Security Controls for a small business," https://www.securitymadesimple.org/cybersecurity-blog/types-of-security-controls-for-a-small-business, accessed: 2021-06-29.

[90] "CIS Controls Version 8," https://learn.cisecurity.org/cis-controls-download, may 2021.

[91] R. Stone, "Fraud, security, and controls in small businesses: A proposed research agenda," *Journal of Business*, vol. 1, no. 3, pp. 15–21, 2016.

[92] Austria, "Datenschutzgesetz - DSG," 2019.

[93] P. Voigt and A. Von dem Bussche, "The eu general data protection regulation (gdpr)," *A Practical Guide, 1st Ed., Cham: Springer International Publishing*, vol. 10, p. 3152676, 2017.

[94] H. Zwingelberg and M. Hansen, "Privacy Protection Goals and their implications for eID systems," in *IFIP PrimeLife International Summer School on Privacy and Identity Management for Life*. Springer, 2011, pp. 245–260.

[95] M. Hansen, "Data protection by default in identity-related applications," in *IFIP Working Conference on Policies and Research in Identity Management*. Springer, 2013, pp. 4–17.

[96] P. Helper, "Is a GDPR Data Protection Officer Really an Essential Hire?" https://www.privacyhelper.co.uk/knowledge-hub-articles/is-a-gdpr-data-protection-officer-really-an-essential-hire, accessed: 2021-06-08.

[97] C. ISiCO Informationssicherheit, Datenschutz, "Data Protection Management System: Implementation and Optimisation," https://www.isico-datenschutz.de/en/service/data-protection-consulting/data-protection-management-system/, accessed: 2021-06-22.

[98] P. Hill and G. Teley, "Data Protection Management System for GDPR compliance - using COBIT," https://www.teley.nl/wp-content/uploads/ITGN-GDPR-DPMS-1.pdf, accessed: 2021-06-22.

[99] R. Gruppe, "Data Protection Management System (DSMS) - Rucon Gruppe," https://rucon-group.com/leistungen/datenschutzmanagementsystem-dsms/?lang=en, accessed: 2021-06-22.

[100] I. G. UK, "ISO 27001 and the GDPR," https://www.itgovernance.co.uk/gdpr-and-iso-27001, accessed: 2021-06-22.

[101] ——, "What is ISO 27701?" https://www.itgovernance.co.uk/iso-27701, accessed: 2021-06-22.

[102] ISO/IEC, "Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and Guidelines," International Organization for Standardization, Geneva, CH, Standard, Aug. 2019.

[103] J. A. Wheeler, "Design Thinking Lies at the Corner of Risk Management and Innovation," https://blogs.gartner.com/john-wheeler/design-thinking-lies-at-the-corner-of-risk-management-and-innovation/, 2016.

[104] K. Sispal, “Design Thinking in Risk Management,” https://kiransispal.com/design-thinking-in-risk-management.

[105] Booreiland, “75 Tools for Creative Thinking,” http://75toolsforcreativethinking.com/, 2019, accessed: 2021-07-02.

[106] “The ”How Might We” Method - Design Thinking Activity,” https://www.odellkeller.com/the-how-might-we-method/, 2019, accessed: 2021-07-02.

[107] J. Courtney, *The Workshopper Playbook - How to Become a Problem-Solving and Decision-Making Expert*. AJ&Smart, 2020.

[108] “Definition - What is a Fishbone Diagram?” https://tallyfy.com/definition-fishbone-diagram/, 2021, accessed: 2021-07-05.