DIGITAL IDENTITY

A cyber resilience evaluation of the European digital identity e-commerce requirements

S.O. De Boer

UNIVERSITY OF TWENTE.

Digital Identity

A cyber resilience evaluation of the European
digital identity e-commerce requirements

Final Version Thesis

MSC Computer Science: Cyber Security
MSC Business Information Technology: IT Management & Enterprise Architecture

Faculty of Electrical Engineering,
Mathematics and Computer Science

By

S.O. De Boer

Graduation Committee

Dr. M. Daneva

Prof. Dr. M.E. Iacob

Dr. F.A. Bukhsh

29 November 2021

UNIVERSITY
OF TWENTE.

Abstract

E-commerce is a quickly expanding market, providing millions of clients with the goods and services that they require. However, this expansive growth can also be a drawback. As the turnover continues to increase, so does e-commerce fraud. For example, in 2020, the cybercrime cases reported for e-commerce increased by nearly 50%. This could be an early indication that e-commerce has become an appealing target for cyber-criminals. If nothing is done against this, it could chase away genuine buyers and sellers and slowly overtake e-commerce entirely.

To curb the number of cybercrime incidents, the European Union (EU) has proposed a digital identity system aimed to link e-commerce accounts with their owners' identity to improve the traceability of fraudulent activities.EU member states are in turn recommended to create their country-specific systems based on these EU requirements, in addition to their country-specific requirements.

As the identity system is likely to be a prime target of cybercriminals, it is essential to ensure that the system is resilient against cyber-attacks. After all, failure to keep the system protected from cybercriminals could lead to a total failure of the system and possibly even worsen the problem.

This research investigates if the EU requirements are sufficient to protect reasonably against cyber-attacks. It does so based on the ISO 31000:2018 approach for cyber risk management.

Using both a stakeholder- and requirement analysis, we first establish an understanding of the system and assess its vulnerabilities. This assessment applies the Unified Killchain Method to one particular regulation, namely EU regulation 2015:1502. The assessment has identified five vulnerabilities:

- Absent requirements related to the server capacity of the system
- The level of malware defence is not specified
- Absent controls against employees performing malicious activities
- Absent requirements for retracting unnecessary network access of employees
- Re-evaluation of authority organisations is not specified

The risk level of each of these vulnerabilities is assessed using a threat capability assessment approach. The overall conclusion of the assessment is that these are all **high risks** except for the malware defence and authority organisation re-evaluation vulnerabilities. The malware defence vulnerability is considered **very high risk** due to many threat agents being capable of abusing it and its potential impact. On the other hand, the authority organisation re-evaluation vulnerability is considered **low risk** as its impact can be quickly mitigated, and its probability is low.

This research continues by analysing possible treatments. This is done in order to guide those that can address the risks. In order to do this, a risk treatment evaluation and usability analysis are performed. We performed a risk treatment evaluation using the ISO 31000:2018 method to address the vulnerabilities. According to our results, EU member states are recommended to implement five additional requirements to address the vulnerabilities. These are:

- The requirement to contract companies that specialise in emergency server capacity against DDOS attacks;
- The requirement to have a level of malware protection considered adequate by leading security standards;
- The requirement to encourage organisational culture to be actively cyber aware;
- The requirement to periodically re-evaluate employees for signs of malevolent intent;
- The requirement to periodically re-evaluate the system authorisations of employees.

As this research identifies five vulnerabilities, it is clear that the system is not perfectly secure. With four of these being of high risk or above, it can only be concluded that the system cannot reasonably protect against cyber-attacks. This answers the main research question. Adding the suggested additional requirements to the national requirements sets will improve the cyber resilience of the proposed digital identity system. This addition will lead to improvements in the prevention of and protection against e-commerce fraud.

The suggested additional requirements are selected to be usable for governments. This is empirically evaluated with experts in the field by using the Use of Technology (UTAUT) method. Based on the opinion of selected experts, it is found that the suggested additional requirements are likely to be accepted by governments.

This research has several implications. Perhaps, the most important is that when the individual EU member states start their national projects to implement the proposed digital identity system for e-commerce, this research can aid them. It helps by first pointing out that the cyber resilience of the EU requirements is insufficient for direct implementation. Then it helps by pointing out the two contributions of this research: (1) an assessment of the risks embedded in the system and (2) suggested additional requirements to address those risks. Both help the EU member states to understand their projects better and improve the cyber resilience of their national requirements sets. In the end, this will result in an eventual drop in e-commerce cyber-crime.

Keywords: E-Commerce, Digital Identity, Cyber Resilience, European System, Digital Fraud, Cyber-Crime

Preface

In front of you is my master thesis "Digital Identity; A cyber resilience evaluation of the European digital identity e-commerce requirements" to complete my two-year master Computer Science specialization Cyber Security and Business Information Technology specialization Enterprise Architecture & IT Management at the University of Twente. By combining the two studies, the two graduation projects have been merged into one large graduation project.

My student days turned out differently than I had envisioned when I applied for a master study in Cybersecurity. My grandfather, father and sister had fantastic stories about their time on campus. Unfortunately for me, after I found housing on campus in February 2020, the Covid-19 measures came into effect. Thanks to the university with its rapid switch to online education, I have not suffered a study delay. On the contrary, there was even room to start a second study.

Graduating has been a valuable experience in which I was able to apply the knowledge and skills I acquired during my studies in my thesis.

The subject of this thesis stems from my personal interest, the social aspect of which has motivated me enormously. I came to this topic indirectly through the following incident. Around Christmas 2019, the academic community was shaken by the ransomware attack at Maastricht University. Although this incident has received a lot of media coverage, for most people the effects were minor. This is in contrast to other cybercrime attacks such as phishing but also account fraud. These crimes have in common that the identity is difficult to verify. For example, a bank employee can verify a customer's identity, but the other way around, a customer cannot verify the bank employee. This also applies to webshops or e-commerce platforms such as *'marktplaats'* where it is not possible to check with whom you do business. Online deceptions are difficult to prevent, but an improved identification method may deter cybercriminals.

Writing my thesis and thus completing my studies would not have been possible without the support of supervisors, family, and friends. First of all, I would like to thank my supervisor Dr. Maya Daneva for her guidance and feedback, which she always gave me with great pleasure, enthusiasm, and expertise. Her motivation was contagious for me and her pleasant way of guiding helped me to enjoy writing my thesis throughout the entire process. In addition, I would like to thank my second supervisor, Professor Maria Iacob, for her comments that have provided a good addition to my thesis.

I would also like to express my gratitude to Dr. Bukhsh and all participants in the evaluation and validation for their participation and valuable responses. I especially appreciated the feedback from the practical experts.

Finally, I would like to thank the people who are close to me: my parents, my sister, and friends who have helped me substantively but also practically during all phases of my study.

I hope you enjoy reading this thesis.

Sebastiaan de Boer

Index

LIST OF FIGURES

LIST OF TABLES

Chapter 1: Introduction

1.1 Context

For the past two decades, E-Commerce has established itself as a disrupting force in nearly all markets. Customer interest in buying online has caused businesses to overhaul their business model completely to fit this trend. The rise in customer interest for e-commerce is unsurprising as the benefits are plenty. The assortment is larger, the shops are easier to compare, and it is generally quicker to shop online than to shop physically. In the past, one had to go to a shop to buy a product; with the introduction of e-commerce, this is something of the past. Today, almost every product is available online and delivered to the door. Unsurprisingly, this convenience has made e-commerce a huge success, as in 2020, approximately 18% of global retail sales were made through e-commerce [28]. This market share is growing steadily, and with the global corona pandemic, more and more people have become accustomed to it. However, with this increased reliance on e-commerce, it is inevitable that fraudulent people try to abuse it more than ever. With the current e-commerce infrastructure, it is nearly impossible to prevent this as fraudulent people can hide behind anonymity. This, in turn, creates an environment of mistrust between buyers and sellers that suppresses the growth of e-commerce.

There is an initiative by the European Union to reduce this mistrust by creating a system through which sellers and buyers can identify themselves [8]. In this system are the digital identities of the buyers and sellers linked with their physical identities. This creates accountability as fraudulent people cannot start new webshops or accounts with a clean slate for fraudulent purposes. This will limit the impact of fraud on e-commerce, and it will enable the police department to detect and monitor fraud activities.

However, this digital identity initiative is still in its infancy, and the basic requirements for such a system have only just been set out [9]. As such, there are a lot of hitches still present that need to be addressed. For example, the regulation lacks specificity in meeting the requirements, focusing on results rather than means. This research attempts to make a contribution by analysing the cyber resilience of these requirements. Considering the size and impact of the EU system, the digital identity initiative is more at risk of being targeted or attacked by different actors, for example, by criminal syndicates, hacker initiatives, and foreign state-sponsored hackers. Therefore, extensive consideration needs to be given to its resilience against this.

In this thesis, resilience is defined as the capability of the system not only to prevent cyber-attacks from getting a foothold but also to resist those that have been able to gain a foothold. This definition has been chosen based on the security principle of a layered defence, which means that one should strengthen their line of defence but should not rely on a single line of defence.

1.2 Problem Statement

A) System explanation

The overall goal of the system is to improve the traceability of E-commerce identity. The improvement should help to prevent and to tackle E-commerce fraud. The 'Vision letter Digital Identity' by the Dutch State Secretary Drs. R.W. Knops elaborates on this premise [1]. His letter presents a basic idea of how the system should function. This is illustrated in Figure 1.

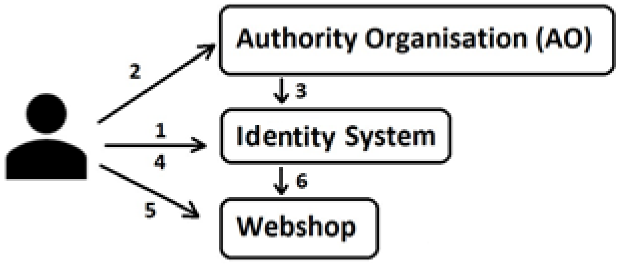


Figure 1: System operation model based on Digital Identity Vision Letter [1]

Figure 1 shows the envisaged basic operation of the system. Four parties are involved in this system: Users, Authority Organisations, the proposed identity system, and webshop platforms. The lines between these parties symbolise an interaction from one party to another, with the number specifying the order in which these occur.

This illustration explains how a user, who wants to make a purchase at a webshop, will do so using the proposed digital identity system. Before making a purchase, the user will need to link it with their account on the digital identity system. If this user does not have this, it will need to create this account with the help of an authority organisation (AO) who can authorise account creation.

The basic operation consists of the following steps. Initially (1), the user sends a request for a new account to the identity system. The system is now aware that a user claims a certain identity and wants to create a new account. However, this claim of identity has yet to be validated. For the second step (2), the user contacts the Authority Organisation (AO) to have his identity validated. The AO has methods to validate someone's identity. This can be done by using DigID, by being physically present with fingerprints or by other methods. The third step (3) sends the AO a confirmation to the Identity system after the claimed identity has been validated. The user can then activate the account (4).

With these steps, a new account is created. When a user creates an account on a webshop or a platform, he/she has to (5) link this account to his digital identity account in the Identity system. In response, (6) the system will confirm that the associated digital identity is a valid identity.

From that moment on, the user can buy and sell on the webshop or platform with a validated identity.

B) Research scope

As mentioned before, this research focuses on the requirements of the EU and the cyber resilience of these requirements. This research assesses whether these are sufficient or whether the EU Member States may need additional requirements in order to be cyber resilient. Figure 2 illustrates the scope of this research. This research does not include architectural models that the individual nations might use for their implementation. The EU member states are, in fact, still making an inventory of which additional requirements they would like to add to their system. Therefore, architectural methods in this study will only be used to illustrate a concept and not to design a system.

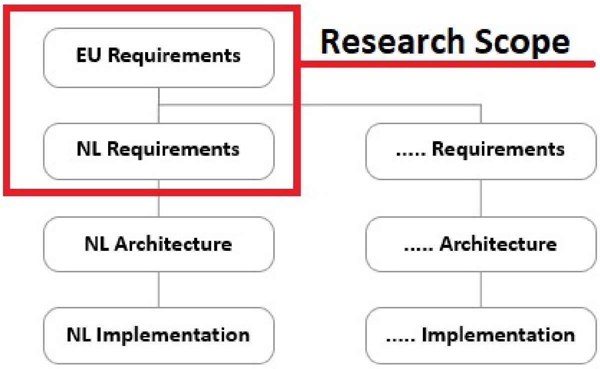


Figure 2: Research Scope Delimitation

1.3 Research Contribution and Relevancy

A) Research Contribution

This research will focus on bringing two contributions. First is an assessment of the cyber resilience when EU regulation 2015/1502 is directly implemented. Second is advice on how national governments of the EU member states can improve the cyber resilience with their own national requirement set.

The cyber resilience evaluation will be recorded in the form of a list of vulnerabilities together with the expected risk they pose. This list concerns the vulnerabilities present when no action is taken by national governments. The advice on how to improve cyber resilience will be provided by giving another list of appropriate approaches for each of the identified vulnerabilities.

B) Research Relevancy

The contribution of this research is primarily relevant to the Dutch government. When writing this research, they are taking the very first steps of creating the system as envisaged in EU regulation 2015/1502. Therefore, this research becomes relevant to them as it provides them with advice on which vulnerabilities could be a problem and how to address them.

Secondary, the study is relevant for other national governments of the EU member states. Similar to the Dutch government, they might have ambitions to join this initiative of the European Union in the future. However, this research does not focus on them as they have not yet decided to allocate resources to achieve this. As such, in the future, the relevance for these governments might become larger.

Lastly, this research has relevancy for e-commerce platforms that want to use the proposed identity system in their account management. As their platforms will rely on the operation of this proposed identity system, they would want to know what risks exist in it. With this information, they will be able to make an informed choice if they should prepare for making their platform interoperable with the proposed identity system.

1.4 Research Framework: the ISO 31000:2018 standard

In order to assess cyber resilience, a scientific approach will be followed according to the ISO 31000:2018 guidelines for risk management. These guidelines prescribe the relevant steps, as seen in Figure 3, to be taken to assess risks and recommend appropriate treatment to those risks.

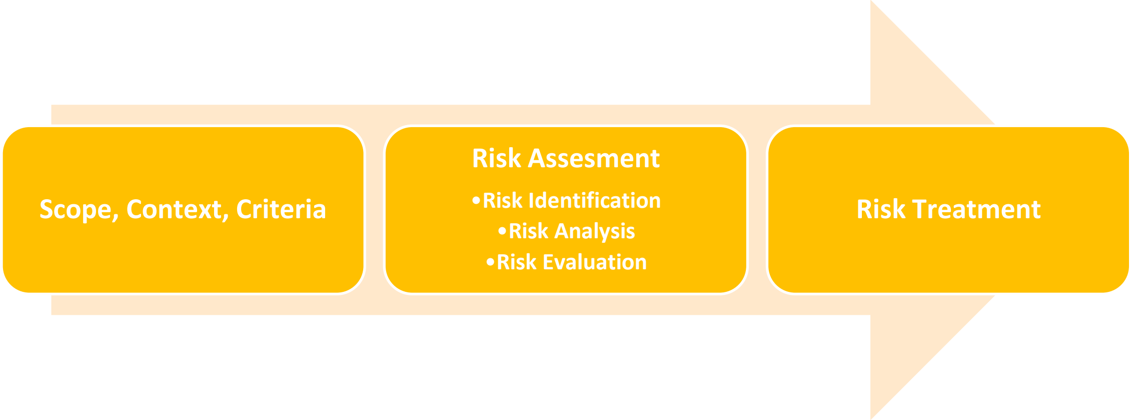


Figure 3: Relevant steps of ISO 31000:2018

Although many competing methods would be suitable for this research, the ISO guidelines proved to be a better fit. This is because ISO describes its methods to be as precise, repeatable, and convincing as possible. Therefore, it is more reliable in its findings as it points out all of the different avenues that could be taken during the realisation, rather than just a selection.

However, this ISO standard only provides the framework for this research. It still needs to be supplemented with other methods. This is because the ISO method is not intended as a stand-alone method. Therefore, additional complementary methods are deployed.

The first step of the ISO method is supplemented by a stakeholder analysis and a systematic literature review. With these methods, the requirements and crown jewels of the system are identified. The second step is supplemented with a vulnerability assessment through the unified killchain method. The last step, the risk treatment, does not require any supplementary method as ISO 31000:2018 already provides a satisfactory method.

1.5 Research Objective and Questions

This master thesis aims to evaluate the cyber resilience of the digital identity initiative based upon the currently published relevant materials. This goal is translated in the following main research question:

> *"Are the currently proposed requirements for an international Digital Identity system for E-Commerce sufficient to reasonably protect the interests of stakeholders against cyber-attacks?"*

The main research question is decomposed into a series of sub-questions that address the different elements of this research problem. The first sub-questions are exploratory and serve problem analysis purposes following Wieringa's design science method [39].

RQ1. *Which stakeholder interests are relevant for the system design?*
RQ2. *What technical requirements are imposed upon the system design?*

Building upon RQ1 and RQ2, the next two sub-questions relate to the cyber resilience of the requirements protecting the stakeholder interests.

RQ3. *What vulnerabilities could arise from the proposed requirements?*
RQ4. *What risks arise from the vulnerabilities in the requirements?*

Based on the findings of RQ3 and RQ4,

a risk estimation has been created. In order to address these risks, an assessment will be performed on possible ways to handle the significant risks.

RQ5. *How can the risks in the design be addressed?*

Afterwards, the results of this study, found in the risk evaluation (RQ4) and risk treatment recommendations (RQ5), need to be evaluated for their usefulness. Proposing new developments without them being deemed useful will not amount to adoption by the relevant stakeholders.

RQ6. *What is the proposed artefact's usefulness perceived by experts in the field?*

1.6 Research Process

In order to answer the research questions, a methodological approach is taken. Figure 4 shows a schematic representation, which follows the design science research framework style of Verschuren & Doorewaard [41]. Therein, the steps are shown that this research follows to answer the sub-research questions formulated in Chapter 1.5.

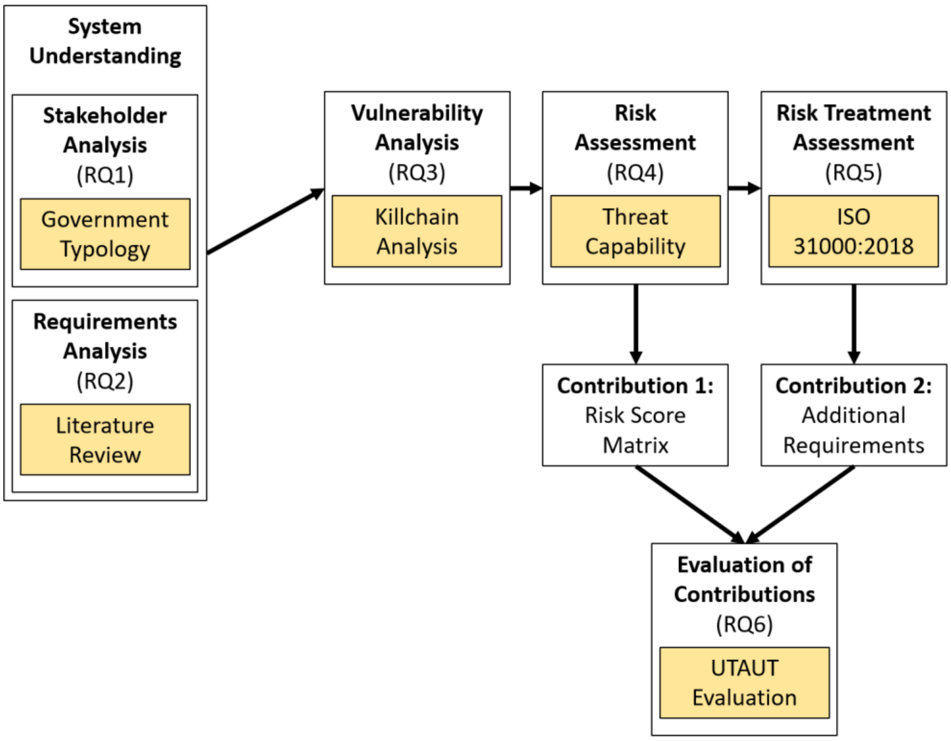

System Understanding
Stakeholder Analysis (RQ1)
Government Typology
Requirements Analysis (RQ2)
Literature Review
Vulnerability Analysis (RQ3)
Killchain Analysis
Risk Assessment (RQ4)
Threat Capability
Risk Treatment Assessment (RQ5)
ISO 31000:2018
Contribution 1: Risk Score Matrix
Contribution 2: Additional Requirements
Evaluation of Contributions (RQ6)
UTAUT Evaluation

Figure 4: Methodological approach

As Figure 4 indicates, the research starts with understanding the system, which will be analysed for vulnerabilities. This is subdivided into (i) performing a stakeholder analysis and (ii) a requirements analysis, respectively addressing RQ1 and RQ2. In yellow, the methods used to perform this analysis are displayed. For performing the stakeholder analysis, a government typology [5] is used. While for the requirements analysis, a systematic literature review [7] is used.

Once the understanding of the system is developed, it is then used in the vulnerability analysis, where a killchain analysis [26] is performed. This results in a list of vulnerabilities which is an input into the risk assessment process. This is done based on a threat capability analysis, where the vulnerabilities are compared to the capabilities of the possible threat agents. Based on the vulnerabilities identified, an assessment is carried out on how risky the vulnerabilities actually are. This is formulated in the first contribution: the Risk Score Matrix. Based on the risks, an assessment of the appropriate treatments is done according to the ISO 31000:2018 standard. This standard prescribes the different manners in which risks can be addressed. In this way, a set of additional requirements is created, which is the second contribution of this research. Both contributions are then evaluated using a UTAUT evaluation [40] to assess their usability. The UTAUT evaluation will answer RQ6.

These steps are expanded upon in section 1.7, where the structure of this research is explained chapter by chapter.

1.7 Thesis Structure

The research questions are described and answered in various chapters. The sequence that is followed arises from the relationship between the various (sub) questions. In addition, the following phases are distinguished: (1) Insight into the proposed project, (2) Evaluation of the cyber resilience, and (3) Suggestions & Validation. The chapters of each phase are found in Figure 5.

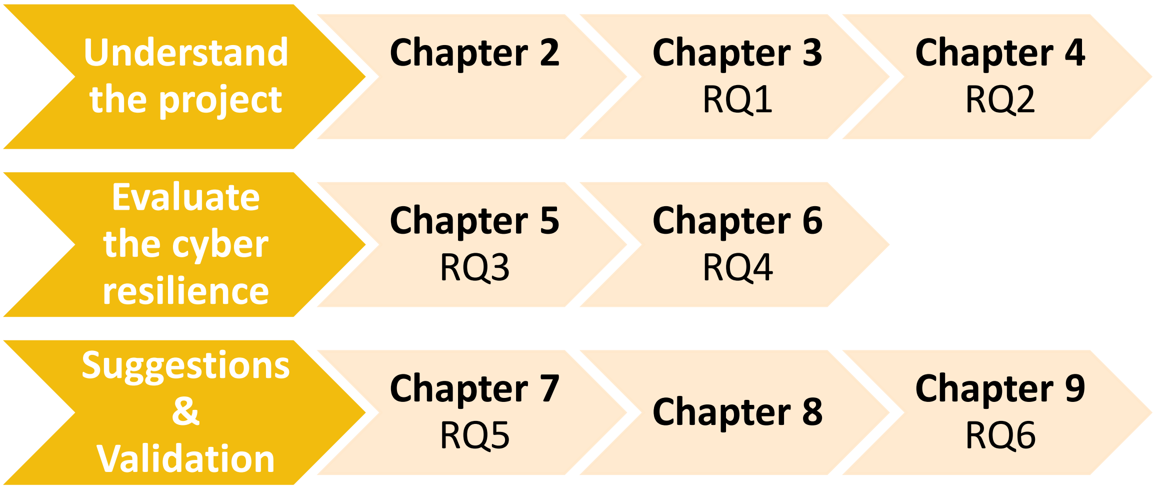


Figure 5: Thesis structure illustration

Chapter 2 deals with the background and related works. This is done by first explaining the current state of the system is, how fear arises from it, and why cybercriminals are interested in exploiting the current system. Current initiatives are considered, and additions to these initiatives are discussed by investigating related works.

Chapter 3 focuses on whom should be considered stakeholders and what their logical drivers are. The stakeholders are identified based on the typology model of Rowly, J [5]. The specific drivers of these stakeholders are identified from a set of common legal, economic, financial, responsible, or ideological drivers. The aggregated results of these drivers will answer RQ1.

Chapter 4 focuses on the requirements for the project. These requirements are identified through a systematic literature review using sources from both academic and legal databases. This results in a set of requirements that explain how the proposed project should work like. Based on this, an ArchiMate model is created to reflect the requirements. This answers RQ2.

Chapter 5 focuses on the vulnerabilities that can arise from the requirements. This is done by applying the unified killchain method of Fox-IT and Leiden University. This leads to a variety of killchains from which the vulnerabilities used are listed. This answers RQ3.

Chapter 6 discusses the risk posed by the vulnerabilities. It does this by first examining the potential threat agents that could exploit the vulnerabilities and their capabilities. This is combined with information on their likelihood to perform these capabilities. Then, based upon this analysis, it assigns a risk level for each vulnerability based on their likelihood and predicted impact. This answers RQ4.

Chapter 7 discusses the possible ways to address the risks as identified in chapter 6 and identify the most suitable response. This will be done by performing a treatment analysis based on the ISO 31000:2018 method. Afterwards, this chapter will give recommendations on how the risks cloud appropriately be handled. These recommendations are the answer to research question 5.

Chapter 8 will describe the validation process and results. It will afterwards discuss options to address the commentary. This validation is performed by an expert review, a variant of the peer review.

Chapter 9 evaluates the contributions of this research with the use of the Unified Theory of Adoption and Use of Technology (UTAUT) method. By doing this, it is estimated how likely the contributions of this research will be accepted based on selected criteria. Together with chapter 8, these two chapters will provide the answer to RQ6.

Chapter 10 focuses on discussing this research results and the limitations. This is based on the individual discussions that were already mentioned in the separate chapters.

Chapter 11 is the conclusion of this research. It will summarise the answers to the individual sub-research questions leading up to the main research question. It will then provide additional findings and make recommendations.

Chapter 2: Background & Related Works

2.1 Background on E-Commerce Fraud

As already touched upon in the introduction, the field of e-commerce is quite expansive. As such, this chapter focuses on making the relevant aspects of E-Commerce and possible fraud cases clear. It does this by first explaining how E-Commerce transactions and then how this creates anxiety for customers. This anxiety is then explained by looking at E-Commerce from a criminology perspective. Afterwards, current EU initiatives are discussed. These initiatives try to address the central issues at the core of E-Commerce fraud. Lastly, other related works to this topic are discussed.

This chapter aids in the creation of contextual knowledge on the topic by discussing all these things, which will help reading the other chapters.

A) Individual sale and purchase.

Currently, the individual sale system works on the basis of accounts. Whenever potential buyers are willing to purchase an item, they need to login into an account. These accounts can often be freely made. During the creation of an account, much information is requested. However, this information is never verified on its accuracy allowing the customer to fill in fake information or even gibberish. The only information that is often verified is the email address. This is usually done by sending an email to the email address given. The email contains a link that verifies the account when clicked. After this, the account is useable for purchases made in the webshop and no further verification is required. To make an online purchase, the customer needs to pay in advance with a selected payment service. The requested item is sent to the customer after payment is received through postal services or mail based on the nature of the item.

B) Platform sales and purchase.

Selling products on a platform is not as universal, however. Some platforms work with verified sellers, which means that the platform controls who is allowed to sell, and the platform guarantees that its sellers are trustworthy. This is the case, for example, with bol.com, which has large numbers of verified sellers. Every seller has a contract with bol.com that allows them to sell their products on the bol.com website.

Other platforms allow anyone to sell at will. This is the case, for example, with marktplaats.nl or ticketswap.nl, which let everyone sell on their platform. Sometimes these platforms require a credit card to be registered where the money is deposited. However, some also offer other payment methods, such as PayPal, without the required registered credit card.

C) How anxiety is created

So, with this system in place, why do civilians fear being scammed through this system? The root of this problem is the fear that one will not receive what one expects to gain as a result of the transaction.

When a potential customer finds a desired product, the customer always pays in advance before receiving the product. As such, there is little guarantee that the product will be delivered. This is in contrast to brick-and-mortar stores where the product is often directly in front of the customer without any form of barrier. The seller will not be able to withhold the item after a successful payment has been made. Even if the item is not immediately in front of the customer on the counter but has to be delivered at a later date, this is less of an issue than when everything is done online. After all, in this case, the customer has a physical address where he can hold someone liable. Online this is much more difficult as contact details such as a physical visiting address are sometimes not or very difficult to find on the website. Further webshops and sellers can disappear and reappear under a different name without any problem.

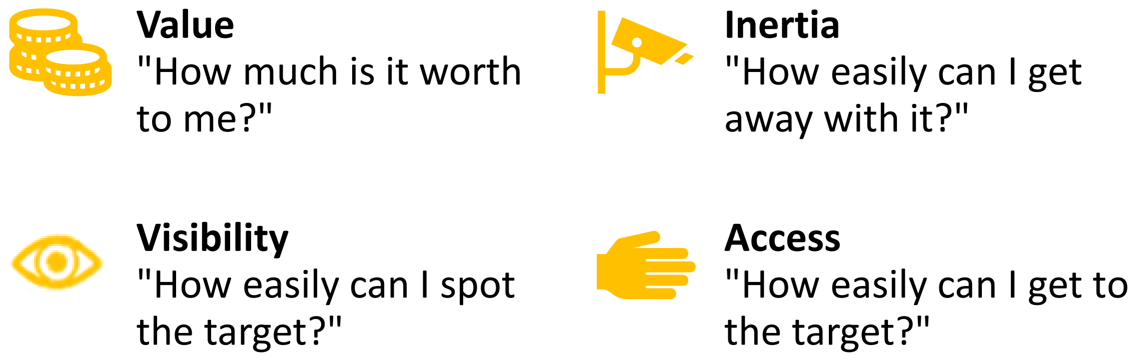
Especially the fact that a seller can disappear and retry under a different name can be a problem for customers. With a system working as explained above, it is clear that creating new accounts is a simple process without having to provide any information that can be used to locate or backtrack the seller or buyer.

This is not only a problem for customers but also for sellers. Since it is very easy for customers to create new accounts that are non-traceable, it is often possible for fraudulent customers to proceed without any form of repercussions. One-way customers can abuse the system is to claim that the product never arrived or to replace a received working product with a broken one and return it. With the ease of recreating customer accounts, non-traceability, and being the initiator of transactions, it is clear that this is a real fear for sellers.

C) Criminal interest in E-Commerce

This fear is not unfounded as globally, around 1.8% of total revenue is lost to e-commerce fraud [29]. Why is e-commerce so attractive for charlatans? A simple answer would be: “because it works”. However, this does not cover everything. Why are frauds choosing to go digital, and aren’t they focussing on other kinds of frauds? An answer may be found from the field of criminology.

According to “Opportunity makes the thief”, criminals tend to choose their target based on four factors: Value, Inertia, Visibility, and Access [30].



Value
"How much is it worth to me?"

Inertia
"How easily can I get away with it?"

Visibility
"How easily can I spot the target?"

Access
"How easily can I get to the target?"

Figure 6: Criminal target selection factors

The expected value of the crime is an important aspect for criminals. A criminal does not perform a crime for the sake of committing a crime. There is always an incentive for the criminal, some reward that they have in mind. This can take many forms, such as monetary gain, goods, reputation or emotional rewards. The criminals might judge different types of ‘rewards’ differently, and as such, criminals may view different things as targets. Bringing this factor into e-commerce, it is clear that this factor is heavily present. There is much money involved in e-commerce, so there is enough value for a criminal to spark interest in this field. Moreover, a criminal could get the desired value relatively easily since it involves direct money or the item of choice.

An important aspect is the perception of the criminal how easily they get away with the crime. In criminology, this is called the inertia aspect. This is a big category because it includes not only how inconspicuous the crime is but also how quickly the crime can happen. When committing crimes, the time in which people are actively engaged in the crime is very relevant because obstacles can arise during that period. In e-commerce, this could be a customer changing his mind during the purchase. The faster a purchase goes, the less likely someone will change his mind. Another reason why slowness is relevant to e-commerce is that it is anonymous, and one can operate outside of the law by operating from another country.

Visibility is a factor relating to how easily a target can be spotted. It is logical that a criminal cannot act upon something he does not know or cannot see. When a wallet is placed in plain sight, it has a higher chance to being stolen than a hidden wallet. This also explains why e-commerce is so viable because criminals encounter it more often, and they might get inspired by it.

Finally, access is the measurement of how easily a criminal expects to reach the target. This is not necessarily just in the form of static defences that make it harder. For example, when criminals start stealing cars, people will buy anti-theft measures that make access harder. In e-commerce, the access factor is quite present. It is easy to start a new account for internet fraud, the fraud schemes are reusable, it has a global range, and if one gets banned, it is easy to restart without much of a hassle.

Based on these factors, it is very clear why e-commerce fraud would be so attractive for charlatans. It has many factors benefitting the criminals and barely gives an advantage for the police. While fraud in e-commerce is not yet fully prevalent, it can easily spiral out of control if nothing is done. Fortunately, some initiatives have already been taken to de-incentivize e-commerce fraud.

2.2 Current Initiatives for addressing E-Commerce Fraud

These issues have also been noticed by governments, who have started to take action to tackle them. This is best illustrated in the letter of the Dutch State Secretary Drs. Knops. He reported on the matter and indicated how the Dutch government launched a project to tackle this issue [1]. This is still in its early developments, only having started initial investigations on this topic. However, this clearly confirms that there is currently an open issue without a solution, at least according to the Dutch government. As such, it has proven itself to be a valid research field with unanswered questions, which became the main source of inspiration for this study.

While this is the most notable of the initiatives, there are more initiatives taken by governments. The most ambitious is the European Union's Electronic Identification Authentication and trust Services (eIDAS) initiative. This initiative focuses on making governmental verified digital identities from different European states, all compatible with each other. This aids in authenticating oneself when dealing with a governmental service of another European Union member state. Due to both its wide-scale of implementation and its similar function, albeit with a different target, it provides technical examples of implementations. Furthermore, this initiative can be used as pre-existing infrastructure to build on.

2.3 Related Works

As mentioned before, the EU regulations 2015/1502 on minimum requirements were already published in 2015 [8]. The regulation entered into force a day after its approval. However, so far, no systems have been realized to which the regulation applies. It appears that the attention to it has been little, up until the Dutch government started its own initiative under the state secretary Drs. Knops [1]. As such, there has also been a lack of academic interest in this regulation.

This is understandable, as yearly, many regulations are adopted by the European Commission for implementation. Not all of these can be the focus of research. Especially when governments have been overlooking it, it could be assumed that researchers would wait until governments have taken action and created a system before researching this topic. With the Dutch government taking the initiative, it is predicted that soon research will start.

However, at the time of writing, there have not yet been published any related sources. For scientific databases such as Scopus, a search for EU regulation 2015/1502 does not yield any search results. Searching for other related regulations would not help in assessing vulnerabilities in EU regulation 2015/1502 and would therefore be irrelevant at this point. However, they do show that there is certainly some interest in researching regulations pursuant to electronic identification.

The implementing regulation EU 2015/1502 is based on parts of EU regulation 910/2014 [8]. The latter regulation is also known as the eIDAS regulation. EIDAS is an acronym for electronic identification authentication and trust services. On eIDAS, research has already been done, such as in "EU regulation of e-commerce a commentary" [37]. This source presents an overview of E-Commerce relevant EU law and provides comments on them. While it does mention the eIDAS regulations, it is not going into much detail on its cyber resilience, focussing merely on the legal aspects that it provides.

If the focus shifts to a less legal approach, papers such as "Towards Stronger Data Security in an eID Management Infrastructure" come into play [38]. However, these only discuss the exact technologies without going into the risks of the system itself. When the focus is on the details of the technology used, a publication is not that useful as the EU Regulation 2015/1502 is not specific with these technologies. Therefore, these would not be so suitable either.

As such, it has to be concluded that this research has no real related works on which it can rely, except the EU law itself. This has been expected already as the Dutch government has only recently started to show attention to it, with other EU member states still ignoring it.

Chapter 3: Stakeholders

3.1 Introduction

When designing or executing a project, the stakeholders and their motives need to be taken into account. But who are the stakeholders? How are they defined? Intuitively one could say that the stakeholders have an interest or concern in the success or failure of a project. But which definition is commonly used in relevant literature?

In this chapter, the term stakeholder will first be defined. After that, the stakeholders of this project and their respective driving motives are identified and analysed. This is based on the interpretation of stakeholder analysis of I.F. Alexander in 'A taxonomy of Stakeholders' [43].

3.2 What are stakeholders

What is a stakeholder? Various sources have tried to define it for a variety of purposes. Unfortunately, this did not result in a convergent definition, but it resulted in various definitions. For example, the following definitions are proposed by different authors:

McGrath, S.K. & Whitty, J. [2]	*"an entity with a stake (interest) in the subject activity"*
Oxford Learner's Dictionary [3]	*"a person or company that is involved in a particular organization, project, system, etc., especially because they have invested money in it."*
Freeman, R.E. [6]	*"any group or individual who is affected by or can affect the achievement of an organization's objectives."*

The differences in descriptions have been the subject of various studies, such as the study by Mitchell et al. [4]. This study found that most scholars try to define the legitimacy of the claims or relationships that would be valid stakeholders [4]. It argues that a potential stakeholder can be confirmed to be a stakeholder if it has one or multiple of the following three attributes:

Mitchell, R.K., Agle, B.R., & Wood, D.J. [4]	*"(1) the stakeholder's power to influence the firm, (2) the legitimacy of the stakeholder's relationship with the firm, and (3) the urgency of the stakeholder's claim on the firm"*

While this definition specifies firms, it is reasonably be interpreted in the context of a project. As such, this is the definition that will be used for this thesis. The reason is that there are a lot of different flavours for defining a stakeholder. However, the best suitable would be the one that focuses on universality, just like this thesis does. It does need to be mentioned that this definition holds no prejudice to the nature of these three attributes. This implicates that one should use this definition to identify stakeholders that want a project to succeed and stakeholders that would oppose a project.

3.3 Who are the stakeholders

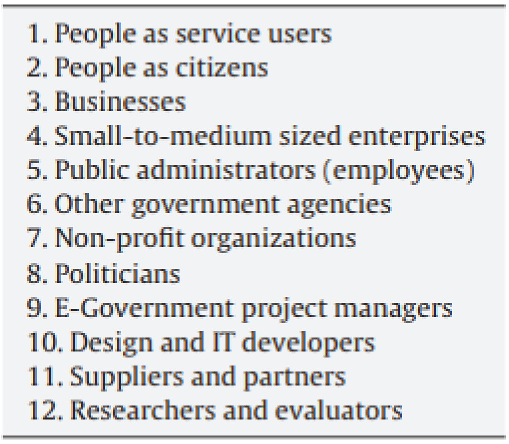
Now that there is a definition of a stakeholder, who are the stakeholders of a universal identification system? An initial direction would be to look towards the reason d'être of this thesis, namely the letter of the state secretary Drs. Knops [1].

The letter of the state secretary of internal affairs has mentioned a series of parties who have a stake in the matter: The Dutch government, cooperating governments, the European commission, knowledge institutions, service providers, identity system providers, international experts, and civilians [1].

This already provides a list of a widespread and diverse number of stakeholders. However, these stakeholders were only mentioned in the letter to support the relevance of specific statements. As such, the letter was not meant to provide an exhaustive list of stakeholders. This means that other stakeholders might be missing in this listing. This raises the question: Is there a reason to assume that the list is not complete?

There is a reason to believe that. As explained in section 2, stakeholders do not necessarily have an interest in the success of the project. The vision letter digital identity of the state secretary Drs. Knops, explains with whom the government is working to define the project. However, it is understandable that such a project would not cooperate with groups opposing its creation. Examples of these would be privacy lobbyists and activists. These have not been mentioned in the letter of the state secretary while they are most definitely stakeholders.

While this example clearly shows that the stakeholder list is not complete, there is no guarantee that it would be complete with this addition. The most feasible method to have some degree of confidence that the stakeholder list is complete would be to use a model in the form of a taxonomy. The model of Rowley, J. on E-government stakeholders, is a good example of such a model [5]. While competing models exist, they do not address a list of possible stakeholders and are applicable to this case. As such, this model will be used to identify additional stakeholders.



1. People as service users
2. People as citizens
3. Businesses
4. Small-to-medium sized enterprises
5. Public administrators (employees)
6. Other government agencies
7. Non-profit organizations
8. Politicians
9. E-Government project managers
10. Design and IT developers
11. Suppliers and partners
12. Researchers and evaluators

Figure 7: Typology of E-government stakeholders as proposed by Rowley, J.

One of the reasons why typologies are so scarce or non-definitive is because there is a wide-scale consensus that stakeholders should be identified on a case-by-case basis by logical deduction. This will be done to find out which of the stakeholders would be applicable from Rowley's typology.

Table 1: Stakeholder Typology Implemented

Nr.	Typology	Suitable?	Specific stakeholders identified
1	People as service users	Yes	Citizens as service users
2	People as citizens	Yes	Citizens as nationals
3	Businesses	Yes	Dutch businesses
4	Small-to-medium sized enterprises	Yes	International businesses
5	Public administrators (employees)	Yes	Police
6	Other government agencies	Yes	Ministry of financial affairs Ministry of justice Ministry of internal affairs European commission
7	Non-profit organizations	Yes	Privacy lobbyists and activists
8	Politicians	Yes	Politicians
9	E-Government project managers	Yes	Identity system providers
10	Design and IT developers	Yes	
11	Suppliers and partners	Yes	
12	Researchers and evaluators	Yes	International experts Knowledge institutions

In addition to the stakeholder mentioned in Table 1, many entities would have a stake in a universal identification system. However, attempting to involve all these stakeholders would result in an over-complicated model, which would not serve the success of this study. Therefore, it is that for this research, the stakeholders who will be taken into consideration will be limited to the stakeholders identified in Table 1.

3.4 Drivers of the stakeholders

Stakeholders are only interested in a project when a project is beneficial in some form to them. So, what are the drivers of stakeholders in this study?

In the letter of the state secretary, the exact goals of each of the stakeholders are not mentioned. This in itself makes sense, as knowing the true drivers of stakeholders is often based on conjecture. After all, stakeholders do not want to disclose anything that could give others a better negotiation position towards themselves. This means that only logical drivers could be deduced. Five types of logical drivers are considered: Legal, Economic, Financial, Responsibility, and Ideological.

Drivers, however, are very subjective. One researcher might identify very different drivers than another researcher. This does not apply to outsiders, but it can also apply within organisations. For example, it is not uncommon that when the leadership in an organisation changes, the change also applies to the drivers of the organisation. Therefore, the focus should be on fundamental drivers that do not change easily unless the research becomes invalidated too quickly. As such, all drivers found must meet one of the following requirements:

(a) Is it fundamental to the purpose of the stakeholder
(b) Is it an opportunity for (in)direct improving its satisfaction of its objective
(c) Is it part of an obligation or right
(d) Does it pose a threat to one of the earlier conditions

A) Legal Drivers

Legal drivers are drivers that aim to fulfil compliance with existing national and international law. As such, legal drivers must be found in international organisations.

The European Commission would have such a legal driver. As part of the obligations that a country accepts when it becomes a member state, it must accept all laws and regulations established by the European Commission. Since an identification system set up by the government would have a significant impact, it is understandable that the European Commission wants to monitor compliance with its laws. As such, a driver of the European Commission would be 'Ensure compliance with European regulations.'

B) Economical Drivers

Economical drivers are drivers that aim to improve the economic situation of an area. The difference with financial drivers is that with financial drivers, the stakeholder benefits directly from it.

This driver can be found at the ministry of financial affairs. This ministry is concerned with the economic development of the Netherlands. With the prospect of universal identification, increasing sales and therefore economic growth, it is obvious that this would be the driver for this ministry to have a stake. As such, a driver of the ministry of financial affairs would be 'Incentivise Dutch economy'.

The European Commission would have a similar driver as the Dutch Ministry of Finance. But, instead, it would focus on the European economy. Hence, the driver would be 'Incentivise European economy'.

C) Financial Drivers

Financial drivers are drivers that are associated with monetary gains. As such, they are especially important for organisations founded with the purpose of monetary gains.

Businesses, both Dutch and international, will have financial drivers for having an interest in this project. A universal identification system would increase mutual trust between parties and increase the number of online transactions. As such, it would provide them with a higher monetary flow. This means that their driver is 'Increasing customer flow'.

On the other hand, identity system providers have a financial driver. The financial benefits to a provider in such a large project would be significant. Furthermore, as contracts are usually also required for maintenance of such a system, it would give them long term financial benefits. This means their driver would be 'Selling and maintaining an identification system'.

Citizens, as users of a service, also have a financial driver. With this project, trust between parties would become less of a problem, and as such, customers would have more options from whom they would like to buy. This means that they can close better deals, and thus they have a financial driver. Therefore, their drivers would be 'More trusted buying options'.

D) Responsibility Drivers

Responsibility drivers are drivers that are related to being responsible for the result. Responsibilities are not necessarily an obligation of result, which means that only failure or success is important. A due diligence approach is often more relevant; a best-efforts obligation. Those who are entrusted with those responsibilities must take preventive action to avoid breaching their responsibility. These drivers are more common in governmental organisations as their right to exist is based on the management of their area of responsibility.

The Ministry of Justice would have such a responsibility driver. It enforces the law, and as such, it should have a natural interest in a system reducing the opportunities for criminals to break the law as it is one of its main reasons for existing. This naturally also applies to the police, which is an extension of the Ministry of Justice. This means that they are both the driver of ‘Reduces opportunities for fraud’.

Another ministry with this kind of driver is the Ministry of Internal affairs. This ministry has the task of gradually improving the quality of life in the Netherlands. As such, they may be interested in this system as it helps to cover this responsibility. Moreover, the aforementioned vision letter of the state secretary was also from this ministry in which this statement was emphasized because they themselves acknowledge it. Therefore, their driver would be ‘Improving quality of life in the Netherlands’.

There is also a type of responsibility with the Ministry of Financial Affairs. While they are mostly driven to incentivise the Dutch economy, this implies that they should be responsible for caring for the economy. In case the project fails or somehow causes problems, they would want to ensure the economy can keep going on. Meaning that they have a driver that is ’Ensure economic continuity’.

Finally, international experts and knowledge institutions also have a responsibility with regard to their research. A universal identification system gives them two motives. First, there is the opportunity to demonstrate the relevance of their research by implementing it into this system. Second, there is the opportunity to open up more research areas with the implementation of such a system. As such, their drivers would be ‘Proving relevancy of research’ and ‘Investigating more research fields’.

E) Ideological Drivers

Ideological drivers are carried by the privacy lobbyists and activists, who will, of course, be concerned about the privacy of this system. After all, a system that, if compromised somehow, would have the potential to leak all private information about its subjects is something of concern. Such a thing is not without precedent, as hackers often target these systems to carry out identity fraud. This concern is also shared to a lesser extent by citizens.

Politicians, on the other hand, would also be motivated ideologically. Politicians have a vision of what a state should look like. As such, politicians could have a vision of digital identity. Some politicians would like to expand the options, while others focus on the risks involved. As such, the driver would be ‘Fitting to political standpoints.’

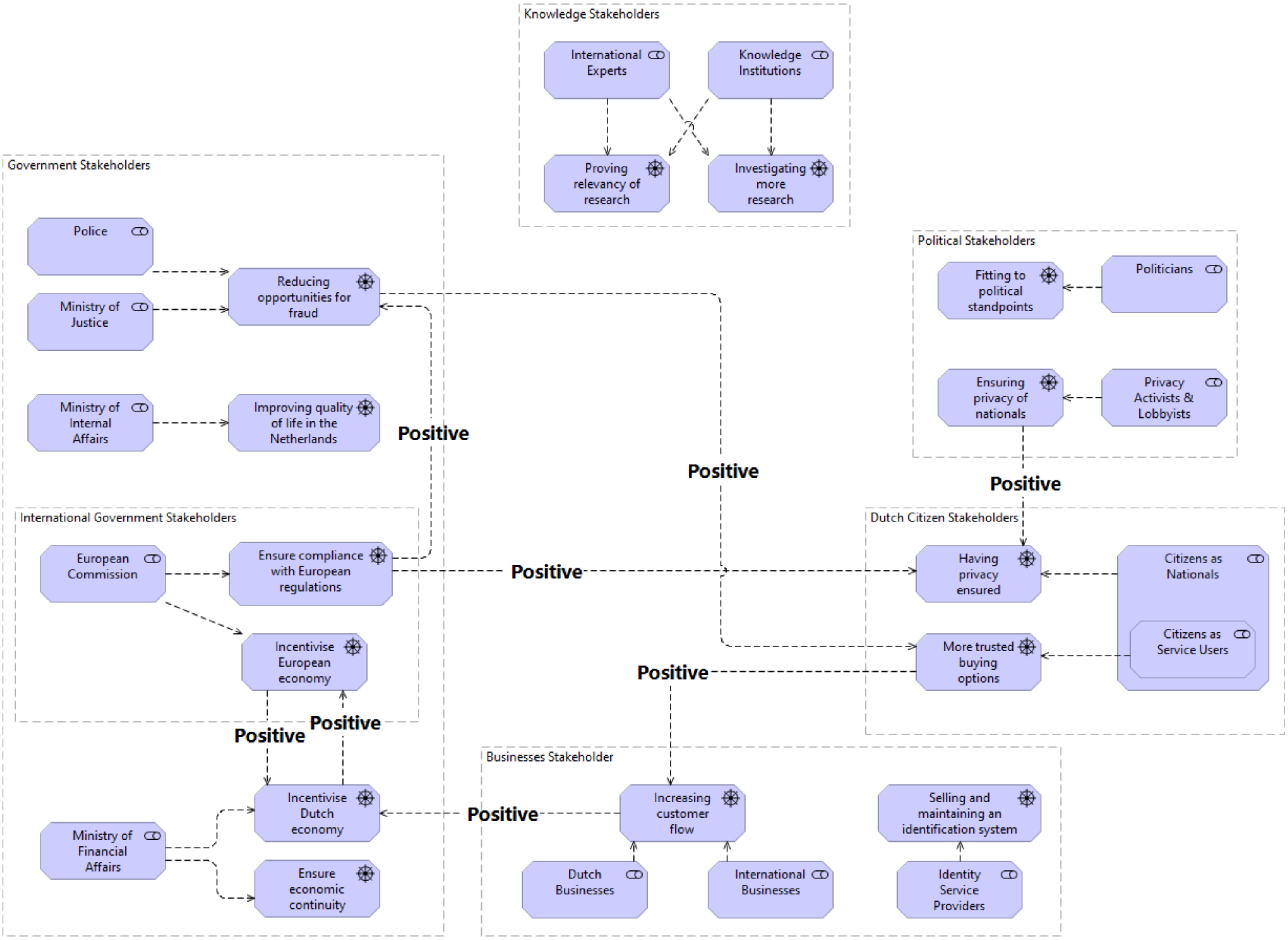
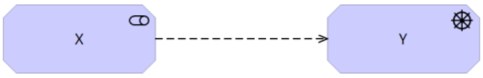
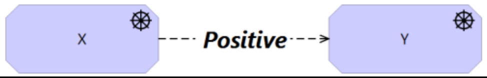

Knowledge Stakeholders
International Experts
Knowledge Institutions
Proving relevancy of research
Investigating more research
Government Stakeholders
Police
Ministry of Justice
Reducing opportunities for fraud
Ministry of Internal Affairs
Improving quality of life in the Netherlands
Positive
Positive
Political Stakeholders
Fitting to political standpoints
Politicians
Ensuring privacy of nationals
Privacy Activists & Lobbyists
Positive
International Government Stakeholders
European Commission
Ensure compliance with European regulations
Incentivise European economy
Positive
Dutch Citizen Stakeholders
Having privacy ensured
Citizens as Nationals
Citizens as Service Users
More trusted buying options
Positive
Positive
Positive
Businesses Stakeholder
Ministry of Financial Affairs
Incentivise Dutch economy
Ensure economic continuity
Positive
Increasing customer flow
Dutch Businesses
International Businesses
Selling and maintaining an identification system
Identity Service Providers

Figure 8: Archimate Stakeholder View Model

Table 2: Archimate Legend of Figure 8

Element	Explanation
	Stakeholder X
	Driver Y
	Stakeholder X influences the driver Y
	Driver X has a positive influence on driver Y

3.5 Analysis

With the many different drivers identified in section 4, it is important to present them graphically. This is done in Figure 8 in a so-called ArchiMate Stakeholder View model. For this, the possible influence that drivers have on other drivers is shown. For example, when more trusted buying options are present, this has a positive influence on the customer flow and therefore also works to incentivise the Dutch economy. Although there might be more relations between the different drivers, the focus was put on preventing over-complexity. The goal is to gain an insight into what stakeholders want and how that connects to what other stakeholders want. A legend of elements and relations is found in Table 2.

The most important observation of this view is that the stakeholders do not seem to have any negative relations between their drivers. This is important as it means that stakeholders are, in fact, not opposed to each other. Therefore, it is possible to satisfy all the drivers as long as resources are available. An implication of this is that, in essence, everyone could be driven towards the success of the project.

Another important observation is the large chain in connections that runs from 'reducing opportunities for fraud' to influence 'Incentivise European economy' eventually. This is important as it means that this driver has a large effect on all the other drivers and, therefore, also on the stakeholders. As such, this might become one of the pillar stones of the study.

The last observation is that there is a group of connected drivers that relate to privacy. Privacy seems to drive many stakeholders, although the connections are not that clearly visible. While in the stakeholder view, it seems to end with having privacy ensured, it goes beyond this. Having their privacy ensured is a driver of citizens as nationals; as such, when this driver seems to do poorly, the support of the citizens will stop. When the citizens do not support the system anymore, they will stop using it. Resulting in a lowered economical effect, which then continues with its driver 'More trusted buying options'. As such, this ensuring privacy becomes the second pillar of this study.

More of these reoccurring patterns exist upon closer inspection. While there are many different ways to group or aggregate the drivers together, a choice has been made to aggregate them in four categories: Trust, Private Data, Economic Continuity, and Economic contribution. Where trust refers to trust in the application and private data refers to the security of this data.

3.6 Conclusion

Although there are a vast number of stakeholders and drivers, it is possible to aggregate the drivers into four categories. These are Trust, Private Data, Economic Continuity, and Economic contribution. These four aggregated categories will be used in chapter 5 as focus areas for vulnerabilities.

Chapter 4: Identification Systems Underlying Mechanisms

4.1 Introduction

In the previous chapter, stakeholders and their drivers have been identified. But how would an identification system satisfy these stakeholders? Or more accurately: What underlying mechanisms should there be in this identification system? In order to answer this question, a Systematic Literature Review (SLR) is performed. This will be done according to the method as set out by B. Kitchenham [7].

4.2 Systematic Literature Review

Before the SLR was performed, some sources that were deemed relevant were examined to discover keywords that could be used to find more relevant sources. It was found that the most notable indicative words were "Electronic Identification" and "Trust Services", especially when both were present. These strings were used in the SLR as a search query. As these terms seemed to both be recurrent in legal and scientific sources, the same search query will be used for both for consistency.

Table 3: Search Query

Legal Perspective **Academical Perspective**	*"Electronic Identification" AND "Trust Services"*

After this search query was used, a variety of sources were retrieved from the databases. As going through all of these sources is not realistic, criteria were specified for selecting which sources to read in more detail.

Table 4: Inclusion / Exclusion Criteria

Inclusion Criteria	
1	Address topics related to mechanisms of an E-commerce digital identity system;
2	Source addresses mechanisms not solemnly inherent to a specific variant of the system.
Exclusion Criteria	
1	Source unavailable in English;
2	Full text of the source is not freely available to University of Twente students;
3	Source is not relevant in EU context.

Sources selected on these criteria were read in more detail, and their value was estimated with a quality assessment. The following questions were considered for the sources to assess their value for this research:

- Did the content of the source reflect what was portrayed in the title and abstract?
- Did the source contribute additional information?
- Do the claims have the credibility to make them plausible?
- Is the source clear on its message?
- Does the message fall within the scope of this research?

If these questions are answered with a yes, then the source is taken into account for this research. By performing this search method, a total of 388 sources were retrieved, as seen in Table 5. These were reduced to 41 by applying inclusion/exclusion criteria. After applying the quality assessment questions, these were reduced to 13 sources.

Table 5: Number of sources during process

	Search Query	**Criteria**	**Quality Assessment**
EUR-Lex (Legal perspective)	100	30	6
Scopus (Academic perspective)	295	11	7
Total	**388**	**41**	**13**

Most of the sources were quickly excluded with the inclusion/exclusion criteria because they focussed on digital identity systems with a different focus area. In this research, only humans are considered, and for example, digital identity systems for the purpose of tracking livestock animals are excluded from this research.

In the Quality assessment, most of the sources in the legal perspective that were dropped were the result of overlapping with other sources and therefore contributing no additional information. While in the academic perspective, this was the result of not falling within the scope of research.

While it was clear that the legal sources are written by the European Commission and therefore from authors in EU member states, all sources selected by the inclusion/exclusion criteria from the academic perspective were from authors in EU member states at the time the source was written. This implicates that not only are the sources applicable in the EU context, but it also shows that the EU is spearheading development in this area.

4.3 Findings from Legal sources

A) What are the sources?

For the legal sources, a total of six sources are used, two regulations and four trade agreements. The two regulations are the two most prominent sources on digital identity specifications. The trade agreements are used as examples of how seemingly unrelated laws could have an impact on the requirements of this project.

Table 6: Important legal sources

	Document	**Main use**
[8]	*EU Regulation 910/2014*	Presents legislation allowing for the creation of digital identity systems for E-commerce
[9]	*EU Regulation 2015/1502*	Presents technical specifications on the legal requirements
[10]	*Trade Agreement with Canada*	Example of National Treatment and Most Favoured Nation
[11]	*Trade Agreement with Japan*	Additional Example
[12]	*Trade Agreement with Singapore*	Additional Example
[13]	*Trade Agreement with CARIFORUM*	Additional Example

B) EU Regulations

The legal perspective is dominated by the EU regulation EU-910/2014 [8] and relevant secondary legislation related to this regulation. The regulation concerns electronic identification and trust services for electronic transactions in the internal EU market. As such, this fits well within the scope of the present research. The fit is so good that it is understandable that this document appears so often in search results, and few other documents are included. However, this document does not go into technical details on how it should work. This is done by the commission implementing regulation (EU) 2015/1502 [9], which sets out the minimum technical specifications and procedures.

Table 7: Mechanisms identified under EU regulation [9]

Enrolment	
	Application & Registration
	Identity proofing and verification (natural persons)
	Identity proofing and verification (legal persons)
	Binding between the electronic means of natural and legal persons
Electronic identification means management	
	Electronic identification means characteristics and design
	Issuance, delivery and activation
	Suspension, revocation and reactivation
	Renewal and replacement
Management and organisation	
	General provisions
	Published notices and user information
	Information security management
	Record keeping
	Facilities and staff
	Technical controls
	Compliance and audit
Authentication	
	Authentication Mechanisms

This regulation specifies that there are various levels of assurance levels that one can achieve when building such a system and goes on to what those levels mean for different mechanisms. The mechanisms that are identified by this commission are in appendix C, and the shortlist is found in Table 7.

As the difference between natural persons and legal persons might not be clear to the reader; natural persons are individual humans, while legal persons are entities that we have given the legal rights and responsibilities of natural persons [14 & 15]. For example, a legal person can be a school or an organisation. They might be associated with humans, that are natural persons. Legal persons can invoke rights and responsibilities on their own. For example, when a large firm starts a court case, it is the firm itself that goes to court and not the CEO.

This difference is certainly important because companies may merge or separate. This also applies to legal persons who can also merge or split off. However, a natural person stays with the same human being for his entire life. Entirely different approaches might be necessary for both types of persons. This is reflected in the way how the regulation treats their identification mechanisms differently.

C) Trade Agreements

Trade agreements between the EU and foreign states [10-13] are another recurrent source type. These trade agreements varied widely, but no clear-cut connection to the topic at hand could be found. Why is it then that these agreements came up so often in the search queries?

Trade agreements are treaties between states or a group of states. The parties involved set terms on how they will open their internal markets for trade with the other party. As this directly impacts the economy of states, the treaties are often very sensitive topics. Every line of these agreements is debated several times over, and new rules are added to reduce the options for one state to abuse the treaty. Amongst these are the clauses that prevent a state from discriminating against foreign businesses or creating unfair competition in favour of its own citizens or those of other foreign states.

In order to counter this, two possible measures have been devised by the states; Most-favourable-nation and National treatment. The first is insurance that nationals of both states will benefit from the most beneficial trade agreement the other state has given to any other state. For example, if nation A gives nation B lower import tariffs, nationals of nation C, who have a most-favourable-nation treatment with nation A, will have lower import tariffs as well. This has various implications but is mostly used to prevent states from creating legal corridors through international treaties.

The second measure, the national treatment, ensures that the trading rights of nationals of both states are equal. This means that if a national of state A is able to perform an action, a national of state B should be able to perform the same action or an equivalent of it. The EU has a large number of such agreements with states around the world.

What does this mean in practice? When the EU has concluded a trade agreement, including a national treatment provision, with another state, a citizen of that state must also have access to digital identification options. Otherwise, there would be an imbalance between EU citizens and citizens of the state party. It would give a competitive advantage for EU businesses and customers. This is a real situation in cases where trade takes place via a digital platform. It is possible that an exception has been made in the treaty.

The above means that when an identification system is set up, the possibilities of digital identification for non-EU citizens must be taken into account.

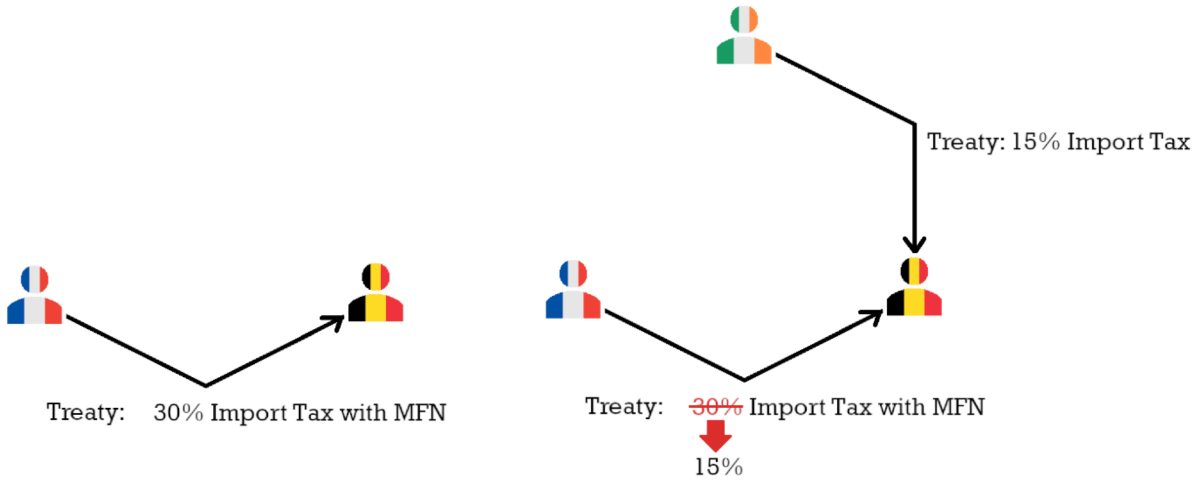

Treaty: 30% Import Tax with MFN
Treaty: 15% Import Tax
Treaty: ~~30%~~ Import Tax with MFN
15%

Figure 9: Most-favourable-nation (MFN) treatment

The second measure, known as the national treatment, stipulates that the trading rights of the nationals of both states are equal. This means that when a national of State A has certain rights, a national of State B is entitled to the same or equivalent rights. The EU has many of these treaties with states around the world.

What does this mean in practice? When the EU has a treaty including this national treatment provision, the nationals of the treaty partner must have access to the proposed digital identity system. After all, if this is not the case, then there is no question of equality but of favouring EU citizens. Companies and customers who have access are maybe considered more trustworthy. Or perhaps companies and customers only buy from or sell to users of this platform.

So, on the basis of treaties with the national treatment, the nationals of the treaty partner must be given access too except in those cases where an explicit exception is made in the trade treaty.

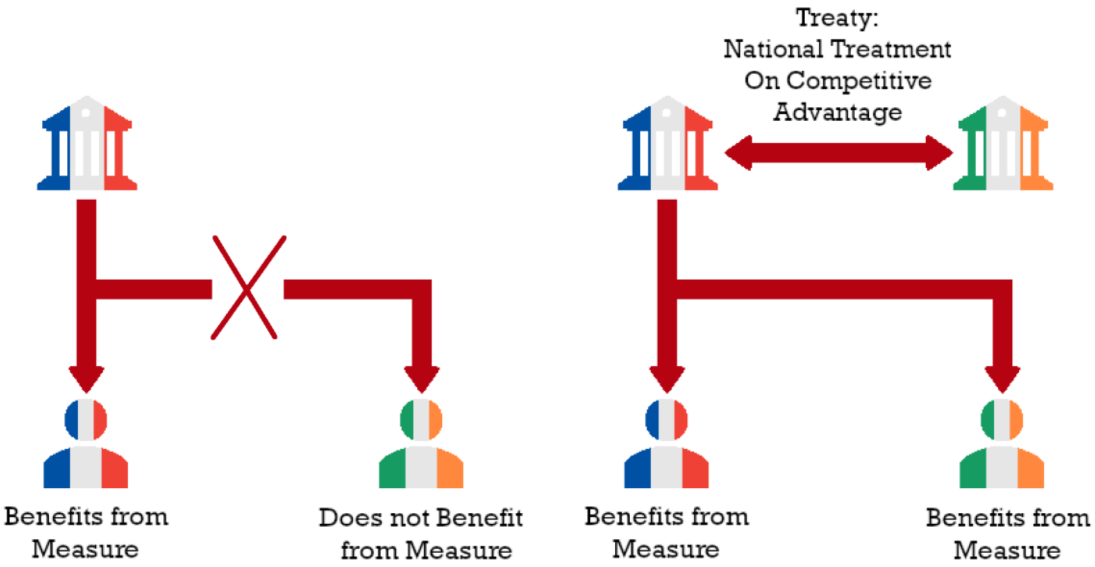


Figure 10: National treatment for non-nationals in government measures giving competitive advantage

This means that a platform should not be created without including a way for non-EU citizens to become a full or equivalent participant. As such, when creating ways for natural persons to establish a digital identity as a user of a platform, there must be a way for non-EU nationals as well to do the same.

4.4 Findings from Academic sources

A) What are the sources?

For the academic sources, a total of seven sources are used. These sources primarily focus on the eIDAS system, as that system shows some similarities to the current project of the EU.

Table 8: Important academic sources

	Document	**Main use**
[16]	*Identification and Trust Techniques Compatible with eIDAS Regulation*	Explain necessity of European Data format
[17]	*Security analysis of EIDAS – The cross-country authentication scheme in Europe*	Explain concept of eIDAS nodes
[18]	*Identity Assurance in the UK: Technical implementation and legal implications under the eIDAS Regulation*	Represent reluctance of states against various forms of standardisation
[19]	*E-identity: Basic building block of e-Government*	Support necessity of European Data format
[20]	*EIDAS as guideline for the development of a pan European eID framework in FutureID*	Explain requirement of usability
[21]	*Moving towards a comprehensive legal framework for electronic identification as a trust service in the European Union*	Explain requirement of evolvability
[22]	*Identity management in cloud computing in conformity with European Union law? - Problems and approaches pursuant to the proposal for a regulation by the European Commission on electronic identification and trust services for electronic transact*	Explain issues relating to national law

B) State Authentication

The academic perspective is focussing primarily on the authentication mechanisms. How should a user be able to prove that he is whom he claims he is? In this, the authors mostly agree that while one single system would be great [21], it is unfeasible for a variety of reasons [16]. For example, some states have a stricter national law on digital identities [22]. If this system is to be implemented for the entirety of the EU, it will become unfeasible to accommodate all of these national regulations. This is especially the case when states sign new laws or even come into conflicting views with other national laws or past experiences with technologies [18]. Some states might already have a digital identity in one form or another and would be unwilling to maintain a second system [17 & 18]. For these reasons, the authors indicate that the most feasible option would not be to create a single method of authentication [16]. But rather a format of authentication, allowing the states to implement their own methods [16 & 19]. This would ensure that all authentication schemes and methods are interoperable with each other as well as give states the freedom and flexibility they require.

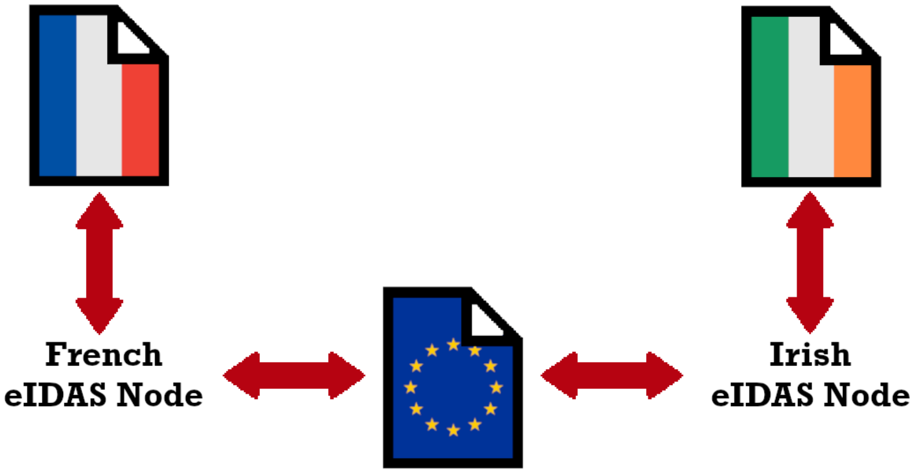


Figure 11:eIDAS nodes translating National Digital Identity formats into each other

In Figure 11, an example is given of how this currently works in eIDAS [17]. Every state has their own digital identity format and allows it to be translated by eIDAS nodes into a universal format. This universal format is then translated into the digital identity format of another state when they require information on a citizen of another state. While it allows for more format diversity, it creates the benefit that each state can adjust its own system without impacting the rest of the system.

C) Authentication Methods

While states are free in authentication schemes, it is stressed that one of the main goals should be usability [20]. Creating a perfect secure scheme is not useful if it is too bothersome to use. For example, if you are only able to prove your identity at a physical location, for example, a bank, then it will be too bothersome for people to use.

While sources provide a variety of options on what states are able to do for this, this would be beyond the scope of this research as this would not be part of a digital identity for E-commerce but of a separate system. However, it does give insight into what options on how authentication of non-EU member citizens would be possible, which would fall into the scope of this research.

The sources indicate that commercial identity providers could play a role in this [18]. After all, unlike states, they are able to provide identities for non-EU citizens. It should be noted that this requires some form of supervision that these identity providers perform their duties with due diligence and attempt to prevent misdemeanours.

D) Evolvability

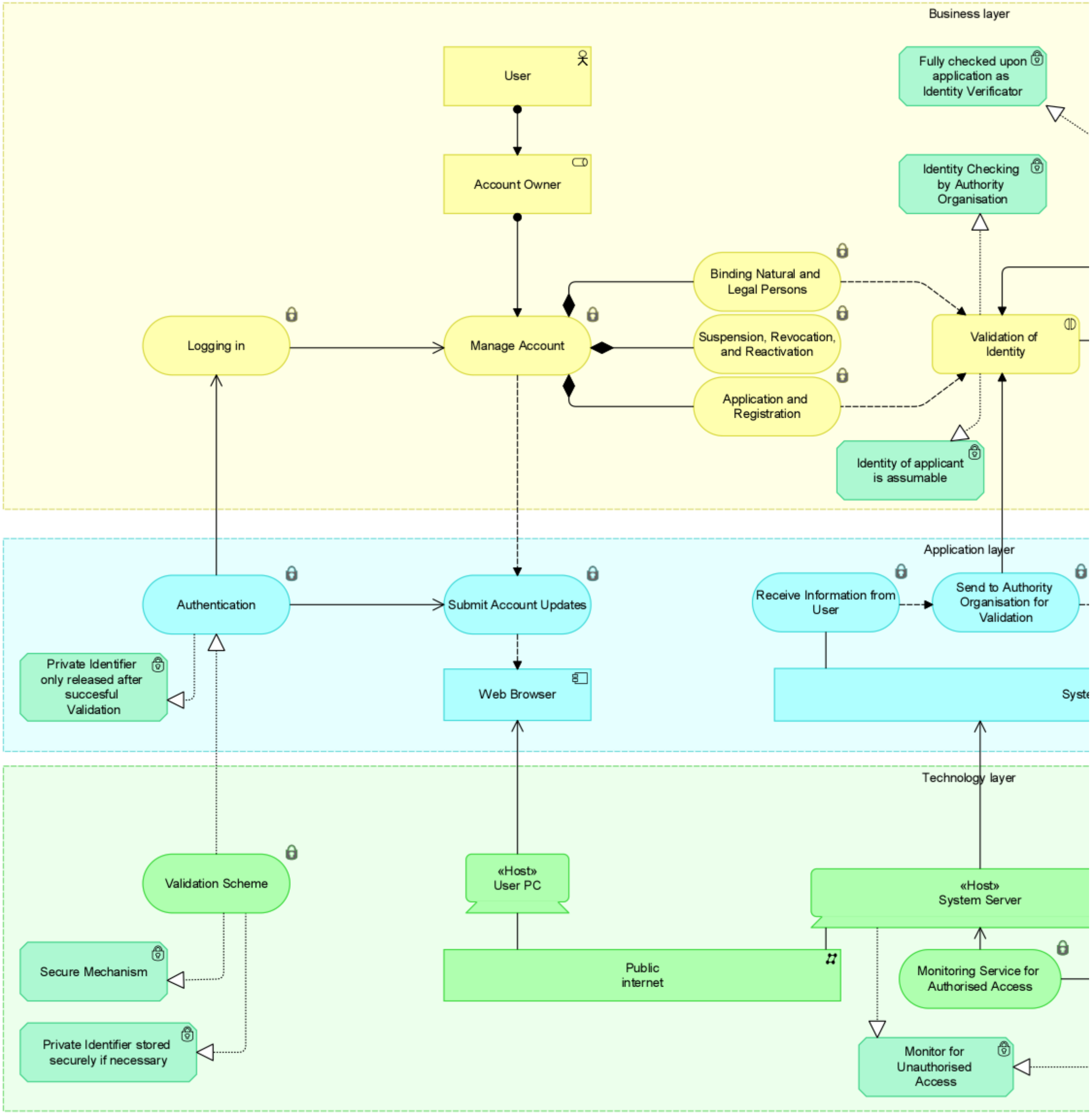
While the main goal for this system would be to be able to connect digital and physical identity, it is possible to use it for more purposes than just identification [16, 20 & 21]. For example, sources state that when a transaction is performed, attaching a timestamp would allow for an increase in traceability. While for example, a digital signature could also be used as a certificate through which the integrity of an agreement could be proven. These options, although not required right now, could become requirements in the future. As such, a flexible framework is necessary in order to ensure evolvability into future adoptions.

4.5 Discussion

By looking at the underlying mechanisms of identification systems from two different perspectives, the legal and academic perspectives, various aspects of Identification systems were explored. Apart from the exact content, some aspects really stood out. For example, most sources seemed to reference back to the legal framework or past projects. For this, there was no distinction between sources from the legal or academic perspective. Furthermore, the sources studied did not mention any other sources not already found in the SLR and that fall within the scope of this investigation. Therefore, it can be stated with some degree of certainty that the most relevant sources are included in this study.

Furthermore, the sources seemed to focus on supplementing existing legislation or existing infrastructure rather than pursuing fundamental changes. This has multiple implications. For example, everyone may agree that the existing infrastructure is the best possible. But it could also mean that authors do not like to challenge the authorities. Whatever the reason, it is clear that neither legal nor academic sources want to change existing regulations or existing infrastructure. Instead, the sources only suggest additions. This means that the mechanisms found in this SLR are not questioned, and as such, the mechanisms can be considered correct and appropriate.

A possible limitation to this SLR is the exclusion of domestic law. As an analysis of Dutch domestic law requires an in-depth knowledge or understanding that only a Dutch Legal scholar could bring, this was not feasible in this research. As such, this forms a limitation as additional requirements could be identified based on domestic law. However, as this research focuses on assessing the cyber resilience of the EU requirements, it would not pose an issue to the validity of this SLR. However, it is a limitation as more potential mechanisms could be identified if domestic law is considered.



Business layer
User
Account Owner
Fully checked upon application as Identity Verificator
Identity Checking by Authority Organisation
Binding Natural and Legal Persons
Suspension, Revocation, and Reactivation
Application and Registration
Logging in
Manage Account
Validation of Identity
Identity of applicant is assumable
Application layer
Authentication
Submit Account Updates
Receive Information from User
Send to Authority Organisation for Validation
Private Identifier only released after succesful Validation
Web Browser
Syste
Technology layer
Validation Scheme
«Host» User PC
«Host» System Server
Secure Mechanism
Public internet
Monitoring Service for Authorised Access
Private Identifier stored securely if necessary
Monitor for Unauthorised Access

Figure 12: Graphical representation of required services according to requirements

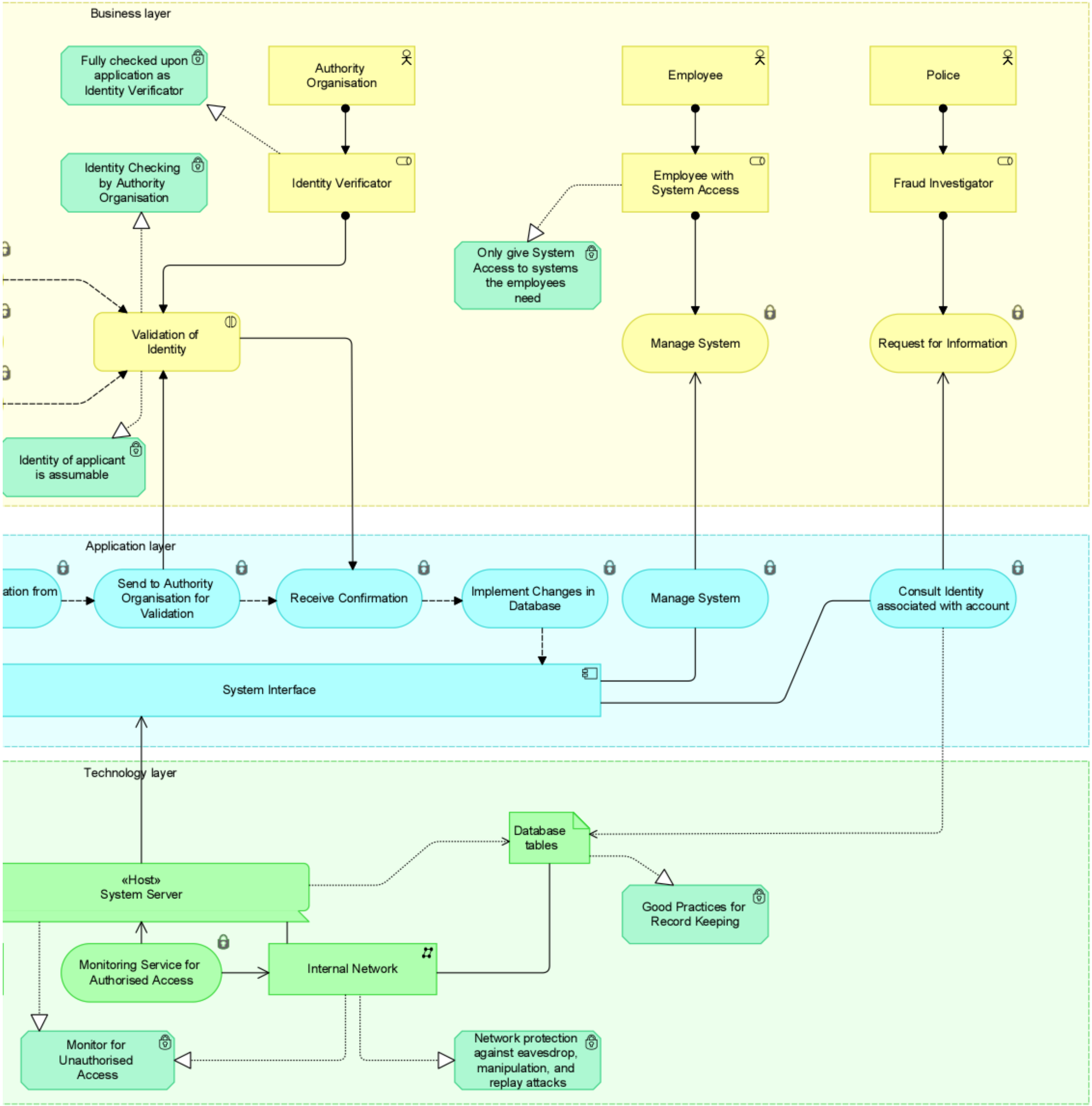

Business layer
Fully checked upon application as Identity Verificator
Authority Organisation
Employee
Police
Identity Checking by Authority Organisation
Identity Verificator
Employee with System Access
Fraud Investigator
Only give System Access to systems the employees need
Validation of Identity
Manage System
Request for Information
Identity of applicant is assumable
Application layer
ation from
Send to Authority Organisation for Validation
Receive Confirmation
Implement Changes in Database
Manage System
Consult Identity associated with account
System Interface
Technology layer
Database tables
«Host» System Server
Good Practices for Record Keeping
Monitoring Service for Authorised Access
Internal Network
Monitor for Unauthorised Access
Network protection against eavesdrop, manipulation, and replay attacks

Figure 12: Graphical representation of required services according to requirements

In Figure 12, a graphical representation is presented of the requirements. As can be seen, most of the elements come from EU regulation 2015/1502. This shows that this source has covered the most notable aspects. This figure is important as it shows from which angles it might be attacked, which will be more relevant in the next chapter. After all, everything that would not require a legitimate actor to interact with directly should, of course, not be accessible. As such, the elements that interact with an actor will have to provide the initial foothold required.

4.6 Conclusion

In this chapter, the underlying mechanisms of identification systems were explored. This was done by performing a systematic literature review on both legal sources and academic sources. The result of this SLR is a set of mechanisms found in Table 7. These mechanisms were supplemented with information on how digital identity can be established. This information will provide the framework through which vulnerabilities can be identified in the next chapter.

Chapter 5: Vulnerabilities

5.1 Introduction

The environment in which the digital identity project is taking place is described in the previous two chapters. Stakeholder requirements, legal requirements, and the requirements from literature can be used to think about the security requirements of such a project. Vulnerabilities need to be identified for this. After all, a risk is only possible if there is a weak point somewhere, a vulnerability.

5.2 Method for Identifying Vulnerabilities

While it would be easy to list a few vulnerabilities and call it a day, this is not the best way to go about doing this. It would not be transparent and not reproducible. As such, it is imperative to apply a methodology that can explain how the results are obtained.

As there is a wide scale of possible vulnerabilities with varying levels of importance, it is necessary to create a framework for these. This is done by looking at the vulnerabilities related to the most important assets of this project, the so-called 'crown jewels.'

Within this framework, a killchain analysis will be performed. There are several options for this, each with its strengths and weaknesses. As such, the process of selecting the right killchain for this approach is explained.

A) Crown Jewels

As stated earlier, crown jewels are the most important assets of a project or organisation. However, the crown jewels are not simply a selection of the most important assets. Rather, they are the essential assets that can cause a project or organisation to fail if they become compromised.

Identifying these Crown Jewels is, in practice, often done by asking stakeholders what they consider important. After all, a project or organisation will fail once stakeholders withdraw their trust. Failing to comply with what stakeholders consider important can lead to them withdrawing their trust. In chapter 3, these have been identified as the drivers of the stakeholders. The aggregation of these will be used as the Crown Jewels for identifying the vulnerabilities. These are Trust, Private Data, Economic Continuity, and Economic Contributions.

B) Lockheed Martin Cyber Killchain

In 2011 Lockheed Martin introduced a new type of model for cyberattacks on targets. The model combines military operational planning expertise with cyber security expertise. This combination would help the modelling of how cyber-attacks occur, allowing to plan against it. The resulting model is a seven consecutive step model of how cyber security attacks happen. These steps are found in Table 9.

According to Lockheed Martin, only when adversaries can go through all of the steps of their model will they be successful in their malign intent [25]. So as long as an adversary can develop a successful killchain, there is a vulnerability. But it works the other way around as well. The defender can place defences preventing abuse by an adversary. Unlike the adversary, the defender only needs to break an attack in one step of the killchain for the attack to fail. After all, an adversary will not be able to skip a single step and, as such, will get stuck, unable to complete his mission.

Table 9: Lockheed Martin Cyber Killchain Steps [24]

Killchain Step	Description
1. Reconnaissance	*“Harvesting email addresses, conference information, etc.”*
2. Weaponization	*“Coupling exploit with backdoor into deliverable payload”*
3. Delivery	*“Delivering weaponized bundle to the victim via email, web, USB, etc.”*
4. Exploitation	*“Exploiting a vulnerability to execute code on victim’s system”*
5. Installation	*“Installing malware on the asset”*
6. Command & Control (C2)	*“Command channel for remote manipulation of victim”*
7. Actions on Objective	*“With ‘Hands on Keyboard’ access, intruders accomplish their original goals”*

C) Mitre ATT&CK Framework

Following the example of Lockheed Martin, various organisations introduced their killchain models to suit their circumstances. Mitre is one of the organisations that did so. The Lockheed Martin Killchain is quite focused on general approaches but hardly goes into the technical details. Because of this, Mitre created an expansive list of techniques that attackers use in the steps. However, this comes at the cost of the simplicity and versatility that the Killchain of Lockheed Martin has. Especially Mitre, which requires a double amount of steps to fit in all the technical details. The steps are found in Table 10.

However, by doing this, Mitre has essentially created a technical shortlist that reduces the blind spot of a practitioner. As such, this method is very useful to inform practitioners of what adversaries are capable of, even when not using this framework as the main framework.

Table 10: Mitre ATT&CK framework steps [23]

Killchain Step	Consists of
1. Reconnaissance	*“… techniques that involve adversaries actively or passively gathering information that can be used to support targeting.”*
2. Resource Development	*“… techniques that involve adversaries creating, purchasing, or compromising/stealing resources that can be used to support targeting.”*
3. Initial Access	*“… techniques that use various entry vectors to gain their initial foothold within a network.”*
4. Execution	*“… techniques that result in adversary-controlled code running on a local or remote system.”*
5. Persistence	*“… techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access.”*
6. Privilege Escalation	*“… techniques that adversaries use to gain higher-level permissions on a system or network.”*
7. Defense Evasion	*“… techniques that adversaries use to avoid detection throughout their compromise.”*
8. Credential Access	*“… techniques for stealing credentials like account names and passwords.”*
9. Discovery	*“… techniques an adversary may use to gain knowledge about the system and internal network.”*
10. Lateral Movement	*“… techniques that adversaries use to enter and control remote systems on a network.”*

11. Collection	*"… techniques adversaries may use to gather information and the sources information is collected from that are relevant to following through on the adversary's objectives."*
12. Command and Control	*"… techniques that adversaries may use to communicate with systems under their control within a victim network."*
13. Exfiltration	*"… techniques that adversaries may use to steal data from your network."*
14. Impact	*"… techniques that adversaries use to disrupt availability or compromise integrity by manipulating business and operational processes."*

D) Flaws in the Killchain Methods

While Lockheed Martin and Mitre's killchain methods have greatly expanded the ability to explain cyber-attacks, they are not flawless. There are still types of cyber-attacks that they are unable to explain. The main flaws lie in that both frameworks falsely assume that adversaries are always from the outside and that no adversary can skip steps [26].

This might be best explained with an example that these killchains have a hard time explaining. Imagine if an employee were to use their own credentials to log into a database and download personal information on clients. It is clear that this would be a vulnerability, but neither killchain is able to describe it. The employee bypasses a lot of steps as the company allows them to. There are flaws in the framework, there is a clear vulnerability but not a way to model it.

These flaws are created by wrong assumptions and could cause major vulnerabilities in a system to be missed. However, with the importance of systems working on continental scale, such vulnerabilities should not be overlooked. Fortunately, these flaws in the frameworks were already identified by researchers around the world, and solutions have been presented. One of these is the Unified Killchain method.

E) Unified Killchain

The University of Leiden and Fox-IT recognised the flaws as mentioned above and decided to solve them by creating their own model [26]. They did this by looking at the designs of a variety of killchain models and unified these designs, something reflected in their naming of the model. However, this model also adds elements of its own to solve the flaws. One of these things is the rejection of the idea that adversaries are unable to bypass steps. This creates a more realistic depiction of reality. As an implication, it also means that cyber security should have security in-depth, meaning that several layers of defence are preferred over a strong single layer. This will be explained in more depth in chapter 6.

As can be seen in Figure 13, the steps of this killchain are grouped together. Although the steps are supposed to be in sequence, it is possible to skip steps if they are not applicable or if one method allows you to switch to another method. In the example from the flaws section, the employee could skip the initial foothold and network propagation entirely as full access is already obtained before starting a killchain.

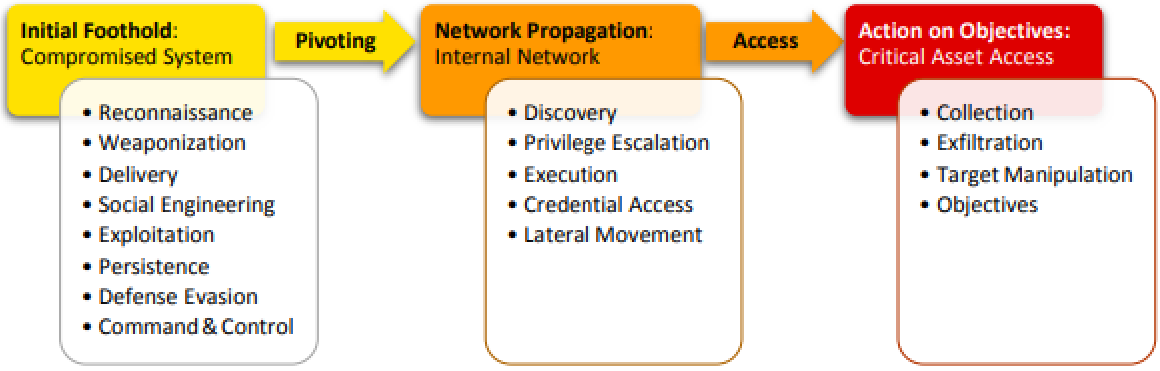


Figure 13: Steps of the Unified Killchain [27]

As this method allows the widest scope of applicability, it will be used to find vulnerabilities. However, as this method does not specify all possible techniques that can be used, it will be used in conjunction with the Mitre framework shortlist. After all, the Mitre framework provides an insightful shortlist that can be consulted to gain insight into possible techniques used by adversaries.

5.3 Results regarding Initial Foothold

The initial foothold [26] has a few options for attackers. These are focused on the different access points for actors. These actors have already been identified in chapter 4: Citizen, Authority Organisation, Business Partner and Facilities & Staff. These could target services primarily focussed around account creation. However, bypassing defences and attacking the internal computers is feasible as well. It is, however, deemed unfeasible to target the authentication mechanisms as it is presumed that an already tested and proven mechanism will be used, making it futile to target.

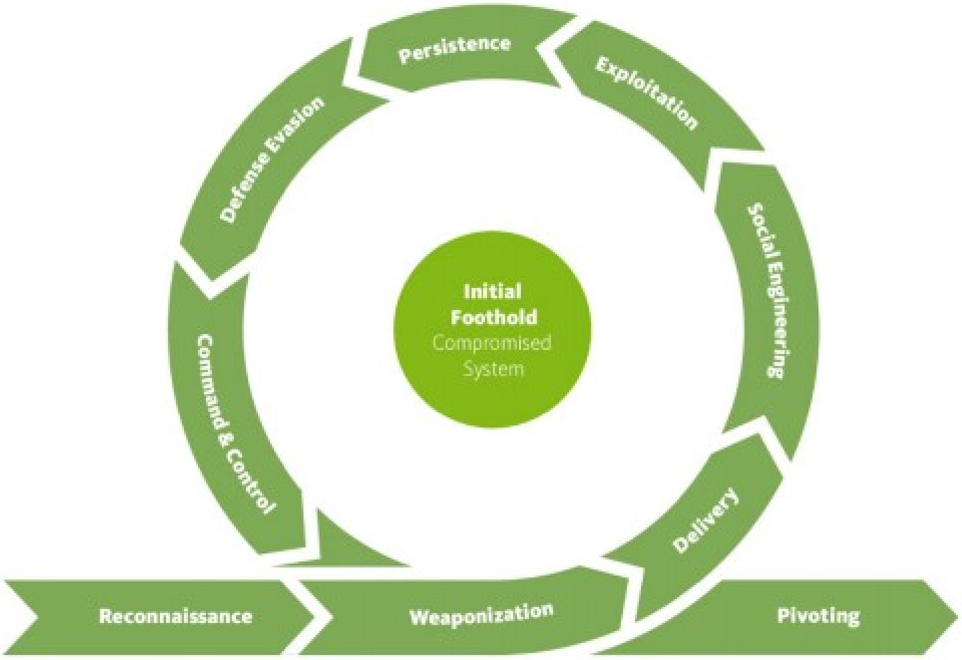


Figure 14: Initial Foothold Steps Unified Killchain [26]

A) Option 1: Full Internet Foothold

This option focuses on gaining a foothold by researching online through open source or leaked files and then targeting the system through the internet gateways. This allows these kinds of attacks to happen regardless of the geographical location of the attacker. It is to be expected that only a zero-day exploit, an exploit that is unknown to the defenders, has a chance of success. Security breaches in major systems are rarely caused by old exploitations as firewalls are constantly updated to protect against them. With this zero-day exploit, it is presumed that this already enables the attacker to constantly communicate with its malware.

Table 11: Full internet foothold steps

Step	**Action**
Reconnaissance	Consulting open sources and leaked files
Weaponization	Buying or developing malware
Delivery	Packets send to open firewall gates / Send email with malware
Social Engineering	- / Convince employee to open email
Exploitation	Zero Day Exploit
Persistence	-
Defense Evasion	-
Command & Control	Communication through Zero Day Exploit

B) Option 2: Internet Service Foothold

This option tries to target the system fully through the internet as well. However, unlike the methods of option 1, this is less sophisticated and instead lays the framework for disruption. It is done by sending fake requests to the services in the hope that at some point, the services fail in their operation and accidentally accept a fake request. The objective can be to create fake accounts, disable real accounts or steal electronic identification means.

Table 12: Internet Service Foothold steps

Step	**Action**
Reconnaissance	Consulting open sources and leaked files
Weaponization	-
Delivery	Send fake requests to services
Social Engineering	Finding out about possible targets through open sources
Exploitation	-
Persistence	-
Defense Evasion	-
Command & Control	-

C) Option 3: Employee Accidentally Providing Foothold

Employees can provide the vulnerabilities that enable an attacker to enter the system. The first way they can do so is by being an unknowing accomplice. This would help in doing the initial reconnaissance and in the delivery and exploitation of the malware. Furthermore, this could help in the latter stages by getting the required credentials as well.

Table 13: Employee Accidentally Providing Foothold steps

Step	**Action**
Reconnaissance	Asking current/past employee
Weaponization	Buying or developing malware
Delivery	Convince employee to plug in USB
Social Engineering	Find unsuspecting employee
Exploitation	-
Persistence	-
Defense Evasion	Zero Day Exploit
Command & Control	Opening firewall gates allowing communication

D) Option 4: Employee Intentionally Providing Foothold

Another option is if that an employee is an active and knowing accomplice. This would allow the attackers to be already deeply embedded in the system before they are noticed. Especially for further steps, this makes detection way harder. However, unlike in other options, keeping anonymous after detection is nearly impossible.

Table 14: Employee Intentionally Providing Foothold steps

Step	**Action**
Reconnaissance	-
Weaponization	Buying or developing malware
Delivery	Plug in USB / -
Social Engineering	Find willing employee
Exploitation	Run malware / Use available employee tools
Persistence	-
Defense Evasion	Covered-up by normal employee activities
Command & Control	-

E) Option 5: Third Party Infection

The system can also be attacked from another direction, namely from a third party. This is possible from the direction of the Authority Organisations. These would have in-depth knowledge of the system and would be able to operate under the disguise of legitimate activities. This would restrict them to focus primarily on account manipulation and creation. How these third parties would be infected or perhaps recruited is a different killchain and, therefore, beyond this vulnerability assessment's scope.

Table 15: Third Party Infection steps

Step	**Action**
Reconnaissance	-
Weaponization	-
Delivery	-
Social Engineering	Learning behaviour patterns of Authority Organisation
Exploitation	Intentional approval of false requests
Persistence	-
Defense Evasion	Disguised by normal activities
Command & Control	-

5.4 Results regarding Network Propagation

After an initial foothold is established, the attackers need to find vulnerabilities that enable them to propagate through the network [26]. After all, with such a large system, it is unlikely that their initial access point is also the objective that needs to be attacked. Not all initial footholds are able to connect to all network propagation options. Therefore, mention will be made which ones are suitable to connect with. Option 2 of the initial foothold is special; however, it does not require any propagation in the internal network as it never aims to be inside of it.

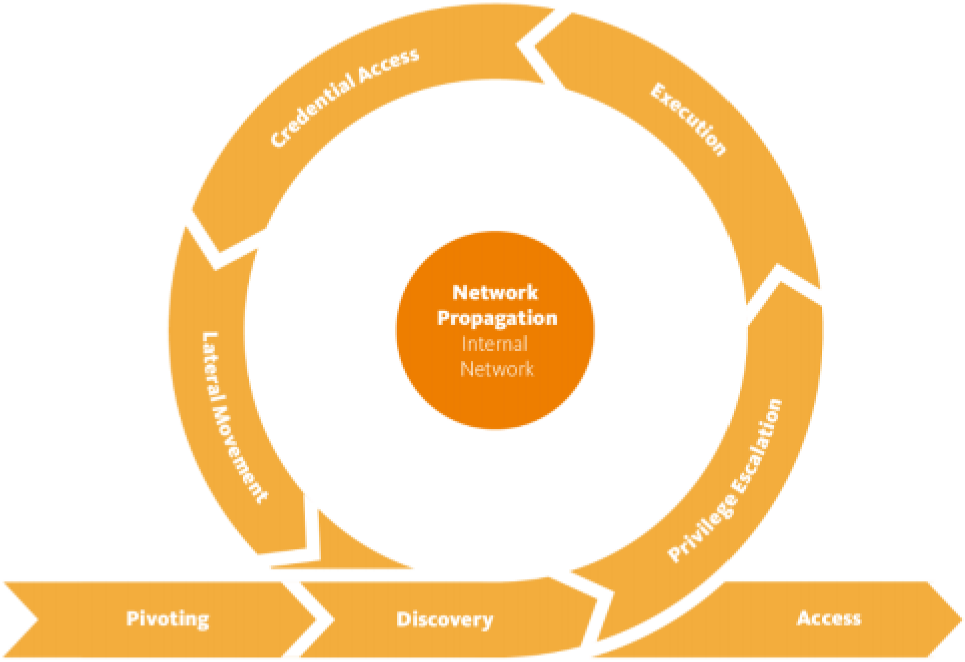


Figure 15: Network Propagation Steps Unified Killchain [26]

A) Option 1: Propagation by Infection

This option focuses on making its way through by mass infecting all possible devices and hoping it will latch onto the right device. This would be suitable for both initial foothold option 1 and option 3. Using information obtained during the reconnaissance, makes it possible for the malware to realise when it is on the right machine. Depending on how covert the adversary finds necessary, it could put strict criteria on which devices to infect. This could lead to only the target being infected.

Table 16: Propagation by Infection steps

Step	**Action**
Discovery	Tracking packet addresses
Privilege Escalation	Recording log-in attempts
Execution	-
Credential Access	Replaying log-in attempts
Lateral Movement	Attaching self to send packages & USB’s

B) Option 2: Employee Propagation

The second option for network propagation is to have an employee spread the malware around. This would allow for precision targeting as the employee knows the system and can bypass outsider defences. This could, for example, be by using the administrative systems themselves. This would be suitable for initial foothold option 4.

Table 17: Employee Propagation steps

Step	**Action**
Discovery	-
Privilege Escalation	Requesting permissions from system administration
Execution	-
Credential Access	Using own credentials / stealing other credentials
Lateral Movement	USB / Email / Administrative Systems

C) Option 3: Approval Propagation

Network propagation can also be done by approving false requests. By doing so, the system accepts changes to its database as a ‘trusted’ organisation approves it. This allows for it to spread to the database of the system. As a result, accounts can be created, and existing accounts can be manipulated. This option is only possible for option 5 of the initial foothold.

Table 18: Approval Propagation steps

Step	**Action**
Discovery	-
Privilege Escalation	-
Execution	Sending & Approving false requests
Credential Access	Using Credentials of Authority Organisation
Lateral Movement	USB / Email / Administrative Systems

5.5 Results regarding Action on Objective

After a malicious actor has done all its preparation and everything is in place, it would need to spring the trap. Just having infected a system means nothing until it comes into action. Of course, these actions would have to match with the previous two phases.

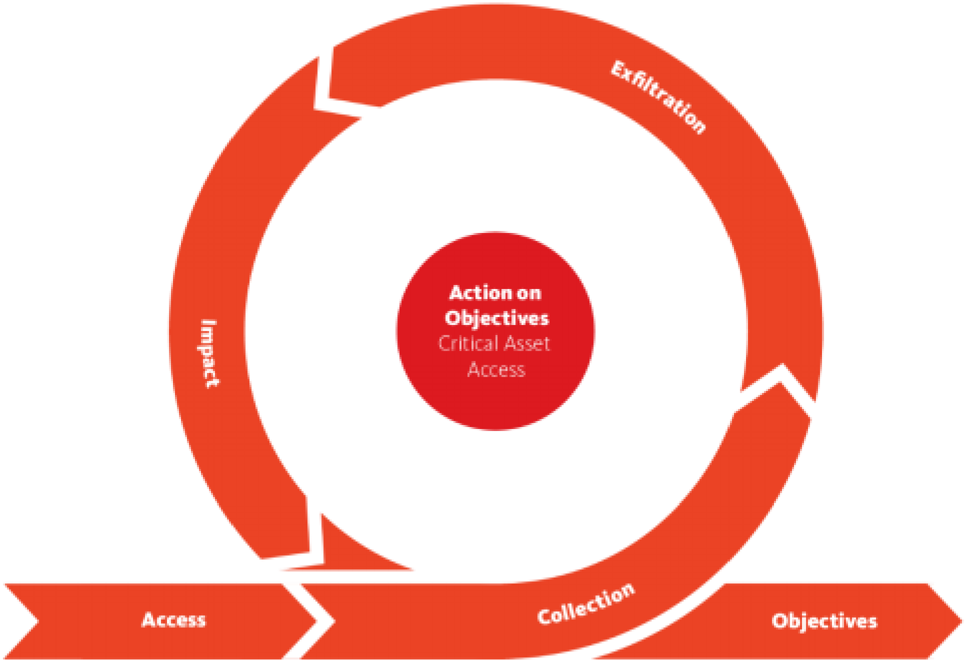


Figure 16: Action on Objectives [26]

A) Option 1: Denial Of Service

This option works by overloading the servers of the system with fake requests. This would prevent the servers from providing any service to users. Any system dependant on the availability of the service would then not function anymore, causing severe economic damage. This option can be taken if, from the initial access, option 2 was taken.

Table 19: Denial of Service steps

Step	Action
Collection	-
Exfiltration	-
Impact	Disable Service with overload of fake requests
Objectives	Short term Unavailable System and dependant third-party webservices

B) Option 2: Destruction of Service

This option focuses on damaging the integrity of the services, thereby making the services themselves non-accessible. It does this by destroying parts of the software infrastructure on the servers. This is only possible with malware actually present on the servers. Therefore, it would require option 1 or 2 of the network propagation.

Table 20: Destruction of Service steps

Step	Action
Collection	-
Exfiltration	-
Impact	Deleting software on servers
Objectives	Long term Unavailable System and dependant third-party webservices

C) Option 3: Infrastructure Crypto locking

This option is comparable to option 2 but less focussed on damaging the infrastructure and more on financial gains. This is done by crypto locking the system and ransoming it. This would only be feasible with option 1 or 2 from the network propagation as it requires malware to be on the servers.

Table 21: Infrastructure Crypto locking steps

Step	**Action**
Collection	Non-specific collection on files
Exfiltration	-
Impact	Crypto locking files
Objectives	Keeping system hostage for ransom

D) Option 4: Data/Technology Theft

This option focuses on stealing technology and data that is available in the database. It would require option 1 or 2 from the network propagation.

Table 22: Data/Technology Theft steps

Step	**Action**
Collection	Collection based on pre-determined demographic
Exfiltration	Send through internet / retrieved through USB
Impact	-
Objectives	Acquiring private data / secret technology

E) Option 5: Fake Account Creation / Manipulation

A malicious actor can abuse the system to target web services that require validated accounts by creating fake accounts or manipulating legitimate accounts. This would aid in disguising malicious acts as legitimate. For this, all three network propagation methods are suitable.

Table 23: Fake Account Creation / Manipulation steps

Step	**Action**
Collection	-
Exfiltration	-
Impact	Accounts created or manipulated suitable for malicious acts
Objectives	Setting up further malicious acts

5.6 Discussion

In this chapter, several options have been discussed which a malicious attacker could abuse. By combining these, the attacker would be able to achieve their objectives and harm the system's crown jewels. As in the previous sections, all steps were mentioned separately and referred to each other. In addition, a simplified graphical overview has been created with the help of the CORAS icons [44]. This can be found in Appendix D. An Archimate model of the vulnerabilities is shown in Figure 17.

When these graphical overviews are consulted, it is easy to see the actual vulnerabilities. This is not always clearly visible from the killchains. Killchains focus on the techniques an attacker would employ to abuse the vulnerabilities in the system. This, however, puts the emphasis poorly. When there are vulnerabilities that can easily be taken advantage of, the killchain is often shorter. This means that the easiest vulnerabilities are often under-represented in the text. While on the other hand, extremely complex and difficult vulnerabilities would require a vast amount of text.

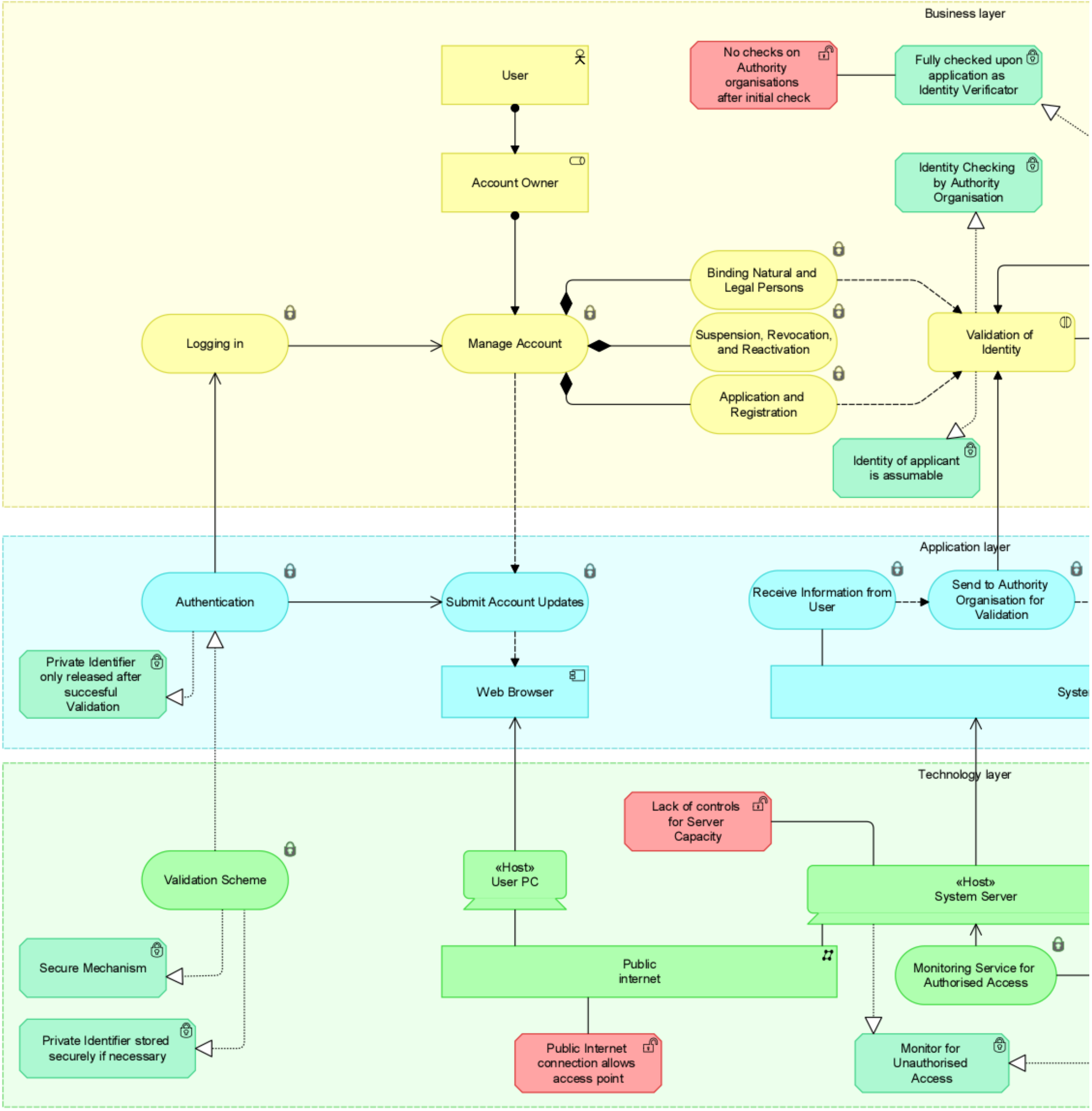
This creates an inverse expectation as a report worth 20 pages explaining a vulnerability seems more pressing than one requiring only two. But, at the same time, the ease with which it can be abused might be the opposite. As such, it needs to be examined what the actual risks are that these vulnerabilities bring. This will be done in the next chapter.

The vulnerability assessment itself gave a set of five possible vulnerabilities. These are: Insufficient server capacity, Insufficient malware defences, Employee disguised malicious actions, Employee access to internal systems, and Deemed trustworthiness of Authority organisations.

An argument that would quickly be pointed out is that some of these are covered in regulation 2015/1502 of the European Union and should not be seen as a potential vulnerability. However, this is based on a misconception. The legislation does not prevent criminal acts. Instead, the legislation allows for the foundation to punish certain behaviours, thereby creating an environment stimulating certain other behaviours. In this case, the legislation would promote adherence to certain technical standards. However, it does not automatically mean that nothing can go wrong. Implementations could be poor, updates delayed, or practices ignored. This could be accidental, but there is also the possibility that this is intentionally by design.

While it might seem impossible to hide intentional disregard for technical regulations on such a massive scale, it is certainly not unprecedented. Volkswagen, for example, managed to hide software manipulating test results in its cars for years. But even in a similar system, this is possible. DigiNotar, previously responsible for maintaining the digital certificates of the Dutch government, has disregarded technical regulations for years until an incident in 2011 [45]. This is very similar to the vulnerability relating to authority organisations.

Therefore, it is clear that there is still potential for vulnerabilities with these regulations. Especially as the regulations still leave a lot of room for manoeuvrability but also vulnerability.


Business layer
User
Account Owner
No checks on Authority organisations after initial check
Fully checked upon application as Identity Verificator
Identity Checking by Authority Organisation
Binding Natural and Legal Persons
Suspension, Revocation, and Reactivation
Application and Registration
Logging in
Manage Account
Validation of Identity
Identity of applicant is assumable
Application layer
Authentication
Submit Account Updates
Receive Information from User
Send to Authority Organisation for Validation
Private Identifier only released after succesful Validation
Web Browser
Syste
Technology layer
Lack of controls for Server Capacity
Validation Scheme
«Host» User PC
«Host» System Server
Secure Mechanism
Public internet
Monitoring Service for Authorised Access
Private Identifier stored securely if necessary
Public Internet connection allows access point
Monitor for Unauthorised Access

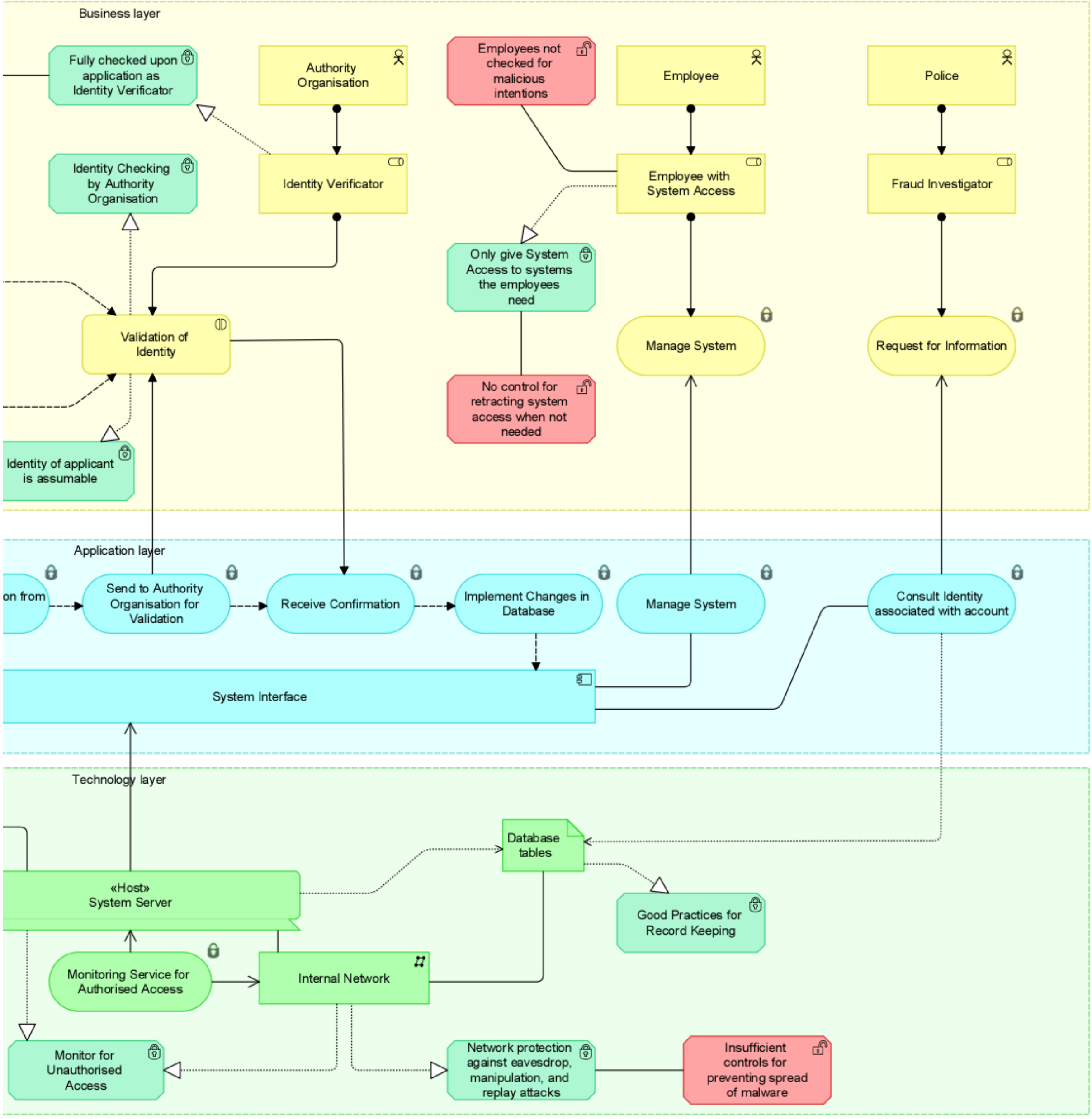

Business layer
Fully checked upon application as Identity Verificator
Authority Organisation
Employees not checked for malicious intentions
Employee
Police
Identity Checking by Authority Organisation
Identity Verificator
Employee with System Access
Fraud Investigator
Only give System Access to systems the employees need
Validation of Identity
Manage System
Request for Information
No control for retracting system access when not needed
Identity of applicant is assumable
Application layer
on from
Send to Authority Organisation for Validation
Receive Confirmation
Implement Changes in Database
Manage System
Consult Identity associated with account
System Interface
Technology layer
Database tables
«Host» System Server
Good Practices for Record Keeping
Monitoring Service for Authorised Access
Internal Network
Monitor for Unauthorised Access
Network protection against eavesdrop, manipulation, and replay attacks
Insufficient controls for preventing spread of malware

Figure 17: Vulnerabilities in EU Regulation 2015/1502

5.7 Conclusion

To conclude, several killchain options have been established. These have led to insight into which potential vulnerabilities exist in the requirements of the system. These are: Insufficient server capacity, Insufficient malware defences, Employee disguised malicious actions, Employee access to internal systems, and Deemed trustworthiness of Authority organisations. This answers sub-research question 3, “*What vulnerabilities could emerge from the proposed requirements*?”

Chapter 6: Risk Assessment

6.1 Introduction

As mentioned in chapter 5, having a vulnerability does not mean that there is a risk. A vulnerability only becomes a risk when there is a chance that someone will exploit the vulnerability. This means that when assessing the risk of a vulnerability, it must be assessed in the context of the threat environment. Therefore, threat agents and their capability to abuse the vulnerabilities must be identified. Subsequently, the actual risks of the vulnerabilities are examined, and an estimate of the risks are made.

6.2 Threat Agents

According to ENISA's 2018 threat landscape report, there are seven significant threat agents [31]. While more kinds of less significant threat agents exist, they are either too rare or pose too little of a threat to be significant. In Table 24, these top threats are listed with a paraphrased description of the group.

It is important to emphasise the aspect of abuse. While many actors are involved in the cyber domain, not all are threats, even when they use them for financial gain. For example, anti-virus businesses make use of the cyber domain for financial gain. However, they do not pose a threat as they protect the cyber domain when used. Therefore, there should be a distinction between those who use the cyber domain and those who abuse it. Nevertheless, the abusers of the cyber domain form a threat.

Table 24: Top Threat Agents as Identified by ENISA's 2018 threat landscape report [31]

Cyber Criminals
Criminals that abuse the cyber domain to gain financial gain
Insiders
Individuals inside a system that are negligent or malicious with cyber consequences
Nation States
States offensively abusing the cyber domain to pursue various agendas
Corporations
Organisations abusing the cyber domain to gain a financial or competitive advantage
Hacktivists
Individuals abusing the cyber domain to pursue a political or social agenda
Cyber Fighters / Cyber Terrorists
Individuals abusing the cyber domain to pursue a religious/ideological agenda
Script Kiddies
Individuals seeking a potential challenge in causing mischief in the cyber domain

These threat agents differ immensely from each other. Some are more common than others, for example. This can be seen in Figure 18, where the motivation for a cyber-attack is cyber-crime by a long shot. This motivation is obviously very connected to cybercriminals. This means that one might encounter thousands of cyber-attacks from criminals each year, but only a handful from nation-states. This, however, does not mean that cybercriminals are, therefore, many times more dangerous than nation-states. Cybercriminals target whom they can, creating a much larger quantity of attacks compared to a nation-state that would focus on quality.

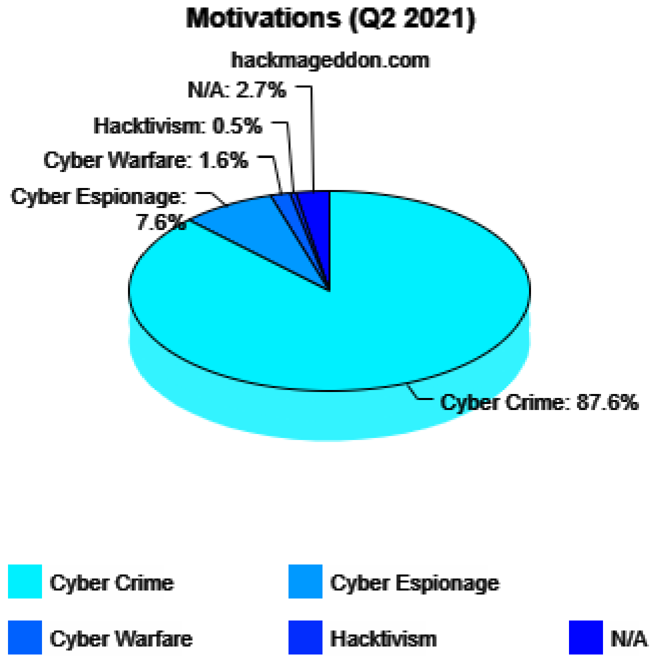


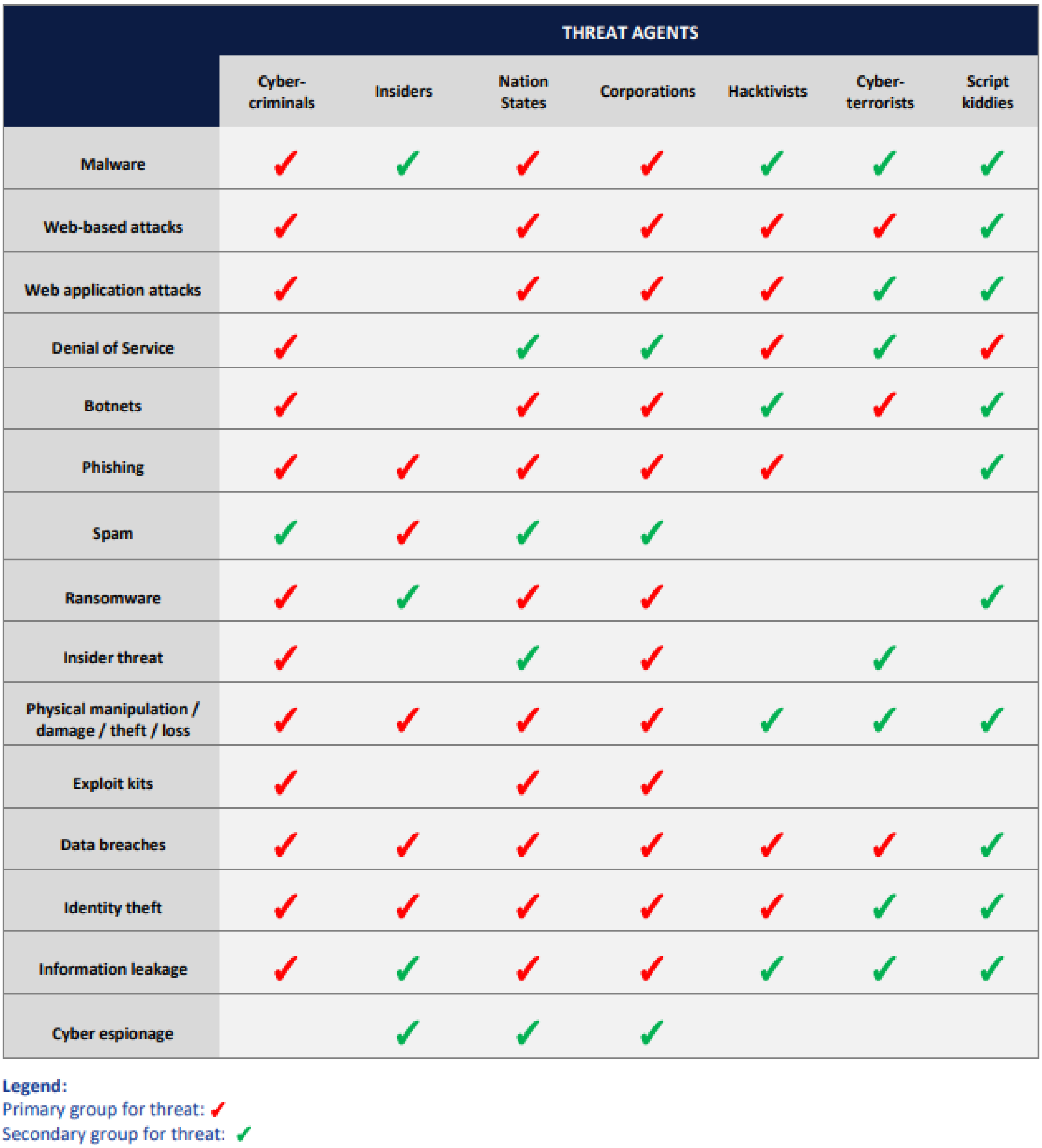
Figure 18: Motivations behind attacks [32]

6.3 Threat Agent Capabilities

The top threats can be very versatile, even within their own categories. For example, one script kiddie can only be capable of Distributed Denial Of Service (DDOS) attacks while another script kiddie can discover new zero-day exploits. The agents that are more active in the cyber domain and therefore come on the radar of cyber security organisations can be so different that they can be uniquely identified based only on their techniques and tools. Though despite this versatility within these categories, each category seems to have its own preferential methods. This knowledge can be used to focus protection against certain types of threat agents.

The reasons for these preferential methods could vary per individual level. However, it is logical that those with access to more resources are more likely to use more sophisticated methods than those who barely have any resources at all. In addition, some methods are more suitable for different types of threat actors. While a script kiddie might be looking for fame and use more visible techniques, a nation-state might prefer more covert methods as not to be held accountable during so-called black flag operations.

For this reason, every type of technique has been assigned to primary and secondary groups in the ENISA’s 2018 threat landscape report. Primary groups refer to the most likely suspects when a technique has been performed, and the secondary groups are possible but less likely. The threat agents who do not belong to the primary or secondary group are considered unlikely to use these techniques. However, it can never be ruled out. The capabilities of each type of threat agent can be found in Figure 19.



	THREAT AGENTS						
	Cyber-criminals	Insiders	Nation States	Corporations	Hacktivists	Cyber-terrorists	Script kiddies
Malware	✔	✓	✔	✔	✓	✓	✓
Web-based attacks	✔		✔	✔	✔	✔	✓
Web application attacks	✔		✔	✔	✔	✓	✓
Denial of Service	✔		✓	✓	✔	✓	✔
Botnets	✔		✔	✔	✓	✔	✓
Phishing	✔	✔	✔	✔	✔		✓
Spam	✓	✔	✓	✓			
Ransomware	✔	✓	✔	✔			✓
Insider threat	✔		✓	✔		✓	
Physical manipulation / damage / theft / loss	✔	✔	✔	✔	✓	✓	✓
Exploit kits	✔		✔	✔			
Data breaches	✔	✔	✔	✔	✔	✔	✓
Identity theft	✔	✔	✔	✔	✔	✓	✓
Information leakage	✔	✓	✔	✔	✓	✓	✓
Cyber espionage		✓	✓	✓			

Legend:
Primary group for threat: ✔
Secondary group for threat: ✓

Figure 19: Threat Agent Capabilities according to ENISA's 2018 threat landscape report [31]

An interesting observation in Figure 19 is that the insider threat agent is not associated with the insider threat capability. It is unclear why ENISA decided to do this. While it could be said that this is a mistake, it is unlikely as it would most certainly have been corrected as ENISA is an official organ of the European Union. With the European Union's commitment to avoid misinformation, this would have been noticed and resolved relatively quickly. With its release dating January 2019, the likeliness of it not having been noticed or corrected if this was a mistake are slim.

A possible explanation for this would be that there is already an insider threat agent in the system. It is therefore not necessary to involve an insider in the system. This is contrary to the assumption in chapter 5 that insiders need their insider capability. The reason for this is that the insider must be in a position where he can perform his malicious actions. For example, a system administrator is in a much better position than a janitor to access the inner cyber domain systems. In essence, while both are insiders, their level of capability to be an insider threat is different. For this reason, it is assumed that this is a capability they implicitly have and should therefore be assumed to be listed in Figure 19 as such.

If the killchain options identified in chapter 5 are mapped to the capability listing, then it would be possible to connect the possible killchains with the threat agents. This mapping is made in Table 25. In Table 26, each variant of the killchain is given an ID to make it easier to reference each variant.

Table 25: Capabilities used in killchain options

Initial Access Point		
1	Full Internet Foothold	Web based attack / Exploit kits / Malware
2	Internet Service Foothold	Web application attack
3	Employee Accidentally providing a foothold	Insider threat
4	Employee Intentionally providing a foothold	Insider threat
5	Third Party Infection	Insider threat / Web application attacks
Network Propagation		
1	Propagation by Infection	Malware
2	Employee propagation	Insider threat / Physical manipulation
3	Approval propagation	Insider threat
Actions on Objective		
1	Denial of Service	Denial of Service
2	Destruction of Service	Data Breach
3	Infrastructure Crypto-Locking	Ransomware
4	Data/Technology theft	Information leakage /Cyber espionage/ Identity theft
5	Fake Account Creation / Manipulation	Identity theft

Table 26: Killchain variants

Initial Access	Network Propagation	Actions on Objective	ID
Full Internet Foothold	Propagation by Infection	Destruction of Service	A
		Infrastructure Crypto-Locking	B
		Data/Technology theft	C
Internet Service Foothold	-	Denial of Service	D
Employee Accidentally providing foothold	Propagation by Infection	Destruction of Service	E
		Infrastructure Crypto-Locking	F
		Data/Technology theft	G
Employee Intentionally providing foothold	Employee propagation	Destruction of Service	H
		Infrastructure Crypto-Locking	I
		Data/Technology theft	J
Third Party Infection	Approval propagation	Identity theft	K

This makes it possible to see how many primary and secondary options each threat agent has. This can help to assess the actual risk each vulnerability poses. After all, when a threat agent has only one possible killchain, and the vulnerability leading to it is solved, then that threat agent has been blocked off as much as possible. However, when a threat agent has many possible killchains, it will be difficult to defend against it as it will change tactics. This means is that the lower the number of alternatives, the more important a particular vulnerability is.

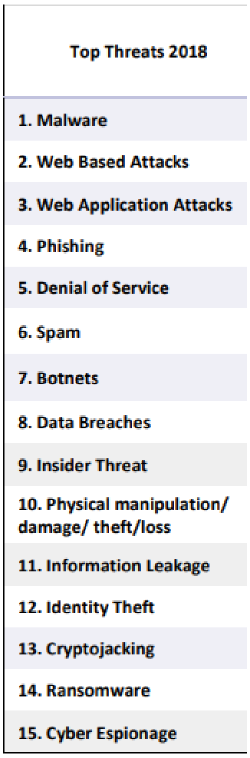
Table 27: Cyber Threat Agents linked to Killchain variants

	Cyber Criminals	Insiders	Nation States	Corporations	Hactivists	Cyber Terrorists	Script Kiddies
A	Primary	Secondary	Primary	Primary	Secondary	Secondary	Secondary
B	Primary	Secondary	Primary	Primary			Secondary
C	Primary	Secondary	Primary	Primary	Secondary	Secondary	Secondary
D	Primary		Secondary	Secondary	Primary	Secondary	Primary
E	Primary	Secondary	Secondary	Primary		Secondary	
F	Primary	Secondary	Secondary	Primary			
G	Primary	Secondary	Secondary	Primary		Secondary	
H	Primary	Primary	Secondary	Primary		Secondary	
I	Primary	Secondary	Secondary	Primary			
J	Primary	Primary	Secondary	Primary		Secondary	
K	Primary	Primary	Secondary	Primary		Secondary	

Table 27 clearly shows that there is a clear distinction in the tenacity of the threat agents. Some, like cybercriminals, can exploit any vulnerability, while hacktivists, for example, have fewer choices in vulnerabilities to exploit. Something that can be inferred from this is that when a full internet foothold or denial of service is not possible, several threat agents lose their primary or even all of their killchain variants.

It should be noted that not all types of attacks are equally frequent. As can be seen in Figure 20, there is a clear hierarchy of attack frequency. Since there are many types of categorisation formats, it is hard to find exact numbers for comparison. Therefore, an estimation of the frequency by ENISA will be used as an indication. It should be mentioned that the figures are taken from a 2018 report, so that the ranking could have shifted a bit since then.

When Figure 20 is compared with the killchain variants and the capabilities used in it, it is clear that the most common type of killchain that threat agents would apply will be A, C, and D. These three killchain variants all have elements that are high on the ranking while for example ransomware and insider threats are noticeably evaluated lower. This gives an indication of what the chance of such attacks is.



Top Threats 2018
1. Malware
2. Web Based Attacks
3. Web Application Attacks
4. Phishing
5. Denial of Service
6. Spam
7. Botnets
8. Data Breaches
9. Insider Threat
10. Physical manipulation/ damage/ theft/loss
11. Information Leakage
12. Identity Theft
13. Cryptojacking
14. Ransomware
15. Cyber Espionage

Figure 20: Ranked top threats according to ENISA's Cyber Threat Landscape report 2018 [31]

6.4 Risk Evaluation

Now that the capabilities of these threat agents are known, the actual risks must be evaluated. This will be done according to the principle that risk is a combination of chance and impact. The logic used for this can be found in Table 28. In this evaluation, the vulnerabilities are assessed in the context of the killchain. The reason for this is that killchains are the symptoms while vulnerabilities are the cause. This evaluation is done in Table 29.

Table 28: Risk level reference table from chance of attack and impact of attack

		Chance of Attack		
		Low	**Medium**	**High**
Impact of Attack	**Low**	Very Low	Low	Medium
	Medium	Low	Medium	High
	High	Medium	High	Very High

Table 29: Risk level of vulnerabilities

Vulnerability	Chance of Attack	Impact	Risk level
Insufficient Server Capacity	High	Low	Medium
Insufficient Malware Defences	High	High	Very High
Employee disguised malicious actors	Medium	High	High
Employee access to internal systems	Medium	High	High
Trustworthiness of Authority organisations	Low	Medium	Low

Insufficient server capacity is considered to pose a high risk of attack as many common threat actors are capable of these attacks. In addition, it is a relatively cheap method of attack as it is possible to hire cybercriminals to carry it out for a fee. However, the impact is considered low as these attacks do not last very long, most of them less than four hours. In addition, it does not have any persistent effect after the attack is finished.

Insufficient malware defence vulnerability is considered a very high risk as it has both a high probability of attack and a high impact. This makes it the highest risk of all vulnerabilities found. The high probability of an attack is because all threat agents can use it in their killchains. Additionally, it is listed as the most common technique used by threat agents, making it highly likely to exploit this vulnerability. Its impact is also considered to be high as it can lead to the destruction of the entire system, possibly leading to its abandonment by its stakeholders. Therefore, this vulnerability is considered a very high risk.

The vulnerability related to employees being disguised as malicious actors is a major risk. With a system of this magnitude, it is inevitable that malicious actors will get through recruitment, or an employee will turn to malicious acts. It is, therefore, better to assume that there are some in the organisation but not to the extent that it goes haywire, making the probability of an attack medium. This is also because, amongst the top attack types, insider threats are halfway on the ranking. While most malicious employees will try to remain inconspicuous and therefore only have a low impact, there will be some who will deliberately attempt to perform actions on a macro scale. Mainly because of the possibility of those types, the impact is treated as high. After all, it can infringe on others or try to destroy the network itself.

The vulnerability related to employee access to internal systems is a major risk. When an employee accidentally carries around malware, there is a good chance that it will infect other computers. However, it does not necessarily mean that when an employee has access to internal systems that he will cause mayhem. Therefore, it is only an average probability of attack. The impact can be detrimental as it can create access points and network propagation for other types of infections. It must be said that some employees need access to internal systems, so this probability can never be non-existent.

Finally, the vulnerability risk related to trust in authoritative organisations is estimated as low. The reason for this is that because the authoritative organisations are external, they are likely to have additional rules and regulations to prevent misuse and to keep the probability of an attack at a low level. Moreover, even if something were to happen, it is possible to revert all changes made by this authority organisation as these will be logged and labelled. As such, the impact is considered to be medium as although it can cause major damage, the damage is repairable.

6.5 Discussion

In this chapter, different techniques have been used to evaluate the risk of each vulnerability. However, this is only one method of evaluating risks. Results may vary depending on the method used. It is expected that the main results of the study will remain unchanged. After all, reproducibility makes risk assessment a science rather than an art.

Another aspect that could influence the results could be that the main source for this chapter, ENISA's 2018 Threat Landscape, is based on data from 2018. Since then, the threat landscape has shifted a bit, making threats different from what they were in 2018. This means that some vulnerabilities might have a higher or lower probability to be abused. Unfortunately, ENISA has not yet released a more up to date version of this threat landscape report as it has shifted format into splitting up its reports. Using these various reports would reduce the uniformity of conventions used to describe the threat agents and capabilities. As such, the choice had been made to choose a source two years old rather than a more recent one that could undermine the clarity of the risk assessment.

6.6 Conclusion

In this chapter, the risks of the vulnerabilities in the requirements are evaluated. It was done by looking at the possible threat agents and their capabilities. This showed that the greatest risk is posed by insufficient malware defences. The subsequent risks are: employees being disguised as malicious actors and employees having access to internal systems. The server capacity is considered a medium risk, and the trustworthiness of authoritative organisations is a low risk. Appropriate responses to these risks will be considered in the next chapter.

Chapter 7: Risk Responses

7.1 Introduction

In the previous chapter, a set of risks related to the requirements for the EU project have been identified. However, identifying and assessing these risks alone would not make sense. It will just become a paper on a desk if no thought is given about what should be done or if something needs to be done at all. Therefore, this chapter addresses research question 5 and asks what suitable responses are for these risks.

7.2 Treatment Options

There is a wide range of options for addressing risks. These can all be derived from one of the basic response options identified by ISO 31000:2018 [33]. ISO has identified seven of these as listed below:

- avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
- taking or increasing the risk in order to pursue an opportunity;
- removing the risk source;
- changing the likelihood;
- changing the consequences;
- sharing the risk (e.g. through contracts, buying insurance);
- retaining the risk by informed decision.

An appropriate response can be selected from these seven for each kind of risk. If necessary, these responses can also be combined in varying degrees to address the risk better. However, some responses are more appropriate than others in certain circumstances. Therefore, the criterium for the different possible treatments are briefly analysed.

A) avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk

This response addresses the risk by cancelling the activity or by not starting in the first place. Which is the most drastic response of them all, but not necessarily uncommon either. The response is most adequate for risks that are impossible to treat cost-effectively and too significant to ignore. This option is considered unfeasible within this project as a cancellation is a political decision and not a requirement.

B) taking or increasing the risk in order to pursue an opportunity

By turning a risk into an opportunity, it is possible to handle the risk differently. Which is especially useful for flexible organisations that can manoeuvre like this. However, it should be mentioned that there exists a chance that the risk will not be converted into an opportunity. For example, increasing the risk in advance by creating a Honey-Pot [34] to attract attackers might cause severe harm instead. An example of how a risk can be turned into an opportunity is that when there is a serious risk of shortage of resources, additional storage capacity can enable an organisation to continue its operations and sell surplus products at high prices.

C) removing the risk source

The risk can be addressed by removing the source completely. This often means eliminating the vulnerability. Unfortunately, this is not always possible, as it may be too complex or unfeasible to completely eliminate the risk. For example, it is very hard to separate and subsequently remove human errors in systems that are used by humans. Even in systems where the source of the risk can be removed, it needs to be assessed whether this is financially suitable. As removing risk sources can be a resource intensive process.

D) changing the likelihood

Risks can be addressed by changing the probability of the attacks. There are several ways to handle this, from technological barriers that prevent the attack to reducing the visibility. Often this is strongly related to the system itself. However, this response option creates one glaring problem. That is often changing the probability is only possible by creating different obstacles. When legitimate users encounter these obstacles, they experience varying degrees of discomfort. As a result, some of them respond by trying to bypass these obstacles so that they will not experience this discomfort. Unfortunately, this means that they create security holes, which can also be exploited by threat agents. An example of this is an employee writing on yellow Post-It notes all his administrative account information in response to systems requiring frequent password changes.

E) changing the consequences

The consequences can also be changed. For example, by changing them into a less harmful variant, reducing the number of consequences or reducing the scope of the consequences. An example of how this can be achieved is to divide a system into sections. Then, when one section of the system is compromised, it does not automatically endanger other system sections. Instead, similar to changing the probability, it tends to create obstacles for legitimate use, making users attempt to bypass them.

F) sharing the risk (e.g. through contracts, buying insurance)

Risks can also be shared. This means that when a risk occurs, the entire burden is not borne by just one organization. For example, part of the consequences can be transferred to an external organisation (e.g. insurance companies).

It is customary that a financial compensation is involved in such an agreement These organisations are often specialised in this field and support multiple organisations in this manner. Sometimes they impose certain requirements on the systems for which they offer insurance. Or they even claim the right to make adjustments to the system security to lower their risk.

G) retaining the risk by informed decision

As the last ‘response’ option, it is possible to accept a risk and decide to do nothing about it. This decision can be made for various reasons, for example, an alternative remedy may be more harmful than the risk itself. Which is especially true for low-risk levels where the remedy costs more than the risk could ever pose. Something to keep in mind is that over time risks tend to change. This means that, as with the other response types, a periodical re-evaluation should be performed.

Table 30: Criteria for choosing treatment

Avoiding the risk by deciding not to start or continue with the activity	
A)	*The activity not essential to crown jewels*
B)	*Alternative options for addressing the risk are not feasible*
Taking or increasing the risk in order to pursue an opportunity	
A)	*Increased risk within acceptable levels*
B)	*Increase in opportunity outweighs increase in risk*
Removing the risk source	
A)	*Risk has a source removable from the system*
B)	*Cost of removing the risk weights up against the risk*
Changing the likelihood	
A)	*Threat agents can be stopped or limited by creating defences*
B)	*The defences do not disproportionally limit the normal use of the system*
Changing the consequences	
A)	*Mitigating factors are possible for the scale of impact*
B)	*Mitigation does not disproportionally limit the normal use of the system*
Sharing the risk	
A)	*Significant risk level but low in likelihood*
B)	*Risk sharing partners available with respect to scale of impact*
Retaining the risk by informed decision	
A)	*Risk is low*
B)	*Average periodical (resource) costs to address are larger than average risk*
C)	*Controls possible for determining when risk changes*

In Table 30 presents a list of criteria for determining which treatments would be feasible options. If a risk satisfies all criteria of a treatment option, then it becomes feasible to choose this option. However as can be seen, criteria like disproportionality or feasibility are criteria that are difficult to pin down. Therefore, these should be carefully decided whether it satisfies it, as it is not as clear cut as other criterion. After this assessment is done for all the treatment options, the most appropriate means are chosen to address the risk.

7.3 Selected Treatments

The risks related to the requirements for the EU project are described in chapter 6. The associated risk levels are given in Table 29. This table is repeated here as Table 31 as a reminder. The possible treatment options, presented in section 7.2, are discussed for each vulnerability in Table 31 in the following paragraphs.

Table 31: Repetition of Table 29 discussing the risk levels of risks

Vulnerability	Chance of Attack	Impact	Risk level
Insufficient Server Capacity	High	Low	Medium
Insufficient Malware Defences	High	High	Very High
Employee disguised malicious actors	Medium	High	High
Employee access to internal systems	Medium	High	High
Trustworthiness of Authority organisations	Low	Medium	Low

Section 7.3.1 starts by looking at the options for the insufficient server capacity vulnerability. Then, the treatment options for the insufficient malware defences vulnerability are discussed in section 7.3.2.

After these hardware/software related topics, the role of an employee is discussed. First as a malicious actor in section 7.3.3 and then in section 7.3.4 as someone who inadvertently poses a risk. The last section looks at vulnerabilities by external organisations.

7.3.1 Absent requirements related to the server capacity of the system

This risk has been noted to occur often but has a relatively low impact. This means that it poses a medium risk to the system. If nothing is done, the system can continue to exist. However, this is likely to increase in attacks as it will become a reliable vulnerability for attackers. So, if it is ignored, it will increase the risk level over time. Due to the frequency with which the attacks are initially expected, any threat agent will be aware of this potential vulnerability.

It is therefore advisable to act against this risk. This can be done by requiring a minimum level of server capacity to handle the load. This would reduce the chance that an attack could overpower this capacity. Although this will likely result in an arms race, in which the attackers will win eventual, as it is far cheaper to attack with a denial-of-service attack than to defend against such an attack [35 & 36]. Moreover, if the requirement is publicly available, like the rest of the requirements, this would tell the attackers exactly how much they need to overpower it. This plays the threat agents right in their hands.

Lowering the consequences is equally difficult. While requirements could be made to mitigate the impact, such as distributing the servers or smart filters, it is likely that the attacking and defending technologies have changed radically in five to ten years. Writing down exact technological requirements will mean that it will create a high standard in the short term, but in the long term, it will become a disadvantage as the system is forced to use outdated technologies. Therefore, it is not appropriate to set detailed requirements.

Turning the risk into an opportunity would be rather far-fetched as there is little gain in server capacity being not available. Removing the risk source is also equally far-fetched. Currently, there does not exist any form of replacement for servers. In addition, removing the threat agent from the equation is also not possible.

Sharing the risk is, however, a very suitable option for this risk type. The risk is created by the sudden increase of network traffic towards the servers. So, the only response is that the server capacity is increased as well. Keeping thousands of servers at hand just in case traffic severely increases is not financially viable, so it is only appropriate to share this risk. When contracts are made with companies that specialise in providing emergency server capacity, the denial-of-service attacks can be handled with a touch of a button. This would keep the risk response both financially viable as well as being able to adapt to changing circumstances. Because the attacks happen frequently but are of low impact, it is possible to revalue contracts if these appear to be non-sufficient for the risk.

Therefore, to handle the risk of insufficient server capacity, it is advised to share the risk by creating the requirement to contract companies specialised in emergency server capacity and use their capacity to counter the denial-of-service attacks.

7.3.2 The level of malware defence is not specified

Insufficient malware defences are considered a very high risk. It scores both high on probability and impact. Being the most common threat, which is and capable of shutting down a system, malware is the most threatening risk of all. Therefore, ignoring this risk is not a possible solution.

Lowering the probability of this risk is a suitable response. It is a common approach for malware as it is somewhat predictable. The response can be keeping anti-virus programs up to date, implementing a layered defence, or creating (physical) air gaps. However, these solutions would have the same problem as mentioned earlier: these security concepts could become outdated. Therefore, it might be helpful to link it to a standard that is continuously updated. This could be phrased as a requirement to have the system achieve and maintain a malware defence level considered adequate by leading cyber security standards.

Lowering the consequences may also be feasible. However, it should be kept in mind that the impact of this risk is a combination of consequences. Therefore, addressing a single consequence will have a minor impact on the total impact. Some options that exist for this risk response are keeping backups up-to-date and compartmentalisation of the system. However, as with reducing the probability, in the long term, it is better to associate this risk response to a security standard that is being updated once in a while.

Turning the risk into an opportunity will be near impossible as it threatens the system’s very existence. Furthermore, the system is not nearly flexible enough to attempt such an approach.

Sharing the risk is possible but probably not worth it. Sharing can be done by contracting external companies that specialise in insuring against cyber-attacks. However, this will likely result in both high costs and only meagre pay-outs in the event of an incident. Moreover, with such a large system, it is even doubtful whether insurance companies can insure this risk. It is therefore not worth defining a requirement for this, especially since money is not the only issue during a cyber-attack. Public perception is just as important, if not more important.

Therefore, the most appropriate way to deal with the risk of insufficient malware protection is to create requirements that require the system to maintain a level of protection against malware considered adequate by leading cyber security standards.

7.3.3 Absent controls against employees performing malicious activities

Malicious employees who are not acting in the interest of the organisation are considered to be a high-level risk. Considering the number of employees involved in the system, it is inevitable that some employees will turn against the organisation. Some might even have joined the organisation with this malicious intention in mind. Therefore, it is not feasible to ignore this risk, and appropriate action should be taken.

Reducing the probability is the most viable option. Two directions could be followed. The first direction is to prevent any employee from becoming a threat agent, and the second is to prevent employee-threat agents from getting into action. The first can be done by regularly evaluating employees for any signs of turning into a threat agent. After all, employees do not change into a threat at random. There might be signs preceding this change. By looking for these signs, it is possible to prevent this change or prevent the employee from causing harm. This is something for which technology cannot help much but where constant human vigilance is necessary. This can be in the form of guiding the organisation's culture or in the form of actual periodical re-evaluation. The second direction that could be taken is by limiting the damage they can actually do. This can be done by limiting employees' access to bare necessities and by using technologies to prevent employees from taking specific actions. However, this is likely going to encourage sharing credentials between employees and bypasses access restrictions. Therefore, an organisational culture that discourages this kind of behaviour would be needed.

Changing the consequences is also suitable for this type of risk. However, with the different types of consequences that can occur, it is difficult to pinpoint what would have the most effect. However, something that would be beneficial in most circumstances would be a way to reverse the consequences. Because many employees work with the system, some may not appear under the radar until it is too late. Therefore, a way to revert the system to a previous state would allow recovery, albeit with downtime and possible data loss since the previous state.

Turning the risk into an opportunity is not appropriate. However, it could be argued that there are opportunities to create so-called 'honeypots' meant to capture and trap attackers before they cause damage. Their usage is often legally questionable and could therefore create a whole new kind of risk to the system.

Sharing this risk is not feasible. The consequences can be so severe that, like the malware risk, it is not really shareable.

Therefore, the most appropriate way to deal with this risk is to create requirements to guide organisational culture towards active cyber awareness. An additional requirement to address this risk is that employees are periodically re-evaluated to see if they pose a threat.

7.3.4 Absent requirements for retracting unnecessary network access of employees

Employees who have access to the internal systems are also considered to be a high risk. While it is only logical that employees should have access to some systems, there is always a risk of accidentally introducing malware. This means that while the negatives cannot be ignored, they cannot be blocked too much either.

One option is to reduce the chance of something going wrong. This can be done by keeping the defences up to date, as explained earlier. However, there are advantages to not relying on a single method. Currently, there are already requirements related to control unauthorised access. However, there is no requirement to re-evaluate who should be authorised and who should not periodically. By re-evaluating periodically, the chance reduces that someone will have access to systems they should not. This risk response can be put into place.

Lowering the impact can be done by following what was explained earlier about the insufficient risk of malware protection, which is compartmentalisation. In short, staying aware of other vulnerabilities will help to protect from this risk. Therefore, no additional requirement is appropriate.

Turning risk into opportunities would be inappropriate because it has such a high risk. However, the chances that things will go wrong and does not become an opportunity are just too high to ignore as well.

Risk-sharing is considered not very feasible. This is because there are simply not enough reasonable risk-sharing options for third parties. Therefore, to mitigate this risk, it is advised to implement a requirement that system authorisation for employees is periodically re-evaluated.

7.3.5 Re-evaluation of authority organisations is not specified

The trustworthiness of authority organisations is considered low risk. It is not expected to happen often, and even if it does, it will not result in the complete destruction of the system. As such, the question can be raised whether this is a risk to be accepted. After all, there are already some requirements that reduce the risks, and the authority organisations will have their own mechanisms to reduce the chance of an incident, in combination with existing national mechanisms to ensure this. If an incident does occur, it is also traceable and can be isolated quickly. Therefore, it may be best to accept this risk for what it is, assuming that authority organisations will act with due diligence.

7.4 Discussion

In Table 32, the findings of the analysis have been summarised. Most of the risks have been addressed, only the trustworthiness of authority organisations being accepted as it is. Although the security of the system would benefit from adhering to these requirements, it is unlikely that all of these recommendations will be formalised as additional requirements.

Table 32: Summary of selected treatment

Vulnerability	Recommendations
Insufficient Server Capacity	Requirement to contract business specialised in emergency server capacity against DDOS attacks
Insufficient Malware Defences	Requirement to have a level of malware security deemed adequate by leading security standards
Employee disguised malicious actors	Requirement to encourage organisational culture to be actively cyber aware.
	Requirement to periodically re-evaluate employees for signs pre-emptive signs of malevolent intent
Employee access to internal systems	Requirement to periodically re-evaluate system authorisation of employees
Trustworthiness of Authority organisations	Accept Risk

The most important reason that not all recommendations will be formalised as additional requirements is that for formalisation of the recommendation, some form of political will is required. A common issue in European politics is that it is often hard to reach a consensus between the different nations. While a form of shared goal exists, it is often closely intertwined with their own agendas. Getting all nations to agree on something would mean finding compromises, which is often a long-term project. Therefore, it could be argued that while these additional requirements would benefit the cyber security of the project, politicians may not be willing to push for them, as this would mean to amend existing agreements and commitments.

However, this would not mean that these additional requirements will not see implementation at all. Based on these requirements alone, it is hard for politicians to justify amendments to agreements. However, when negotiations are already taking place, for example, for budgetary reasons, there is less reluctance also to negotiate an amendment of the requirements.

Another point of discussion, already mentioned in previous chapters, is that some might argue that these are implicitly already part of the requirements laid down in EU Regulation 2015/1502. While it might be tacitly understood by those who created the system, there are no guarantees. It is possible to build a functional system with the current requirements that does not meet the additional requirements. However, this would result in a system highly vulnerable to the risks as mentioned above. Requirements do not exist merely to prevent a flawed system but also to guide the creation of the system. Therefore, when a requirement is not mentioned explicitly, it is prone to be ignored. This does, however, need to be balanced against the need for some flexibility.

7.5 Conclusion

In this chapter, the risks that are identified in chapter 6 are analysed for possible treatment options. This has been done according to the methodology of ISO 31000:2018. As a result of this, five additional requirements have been devised as possible responses to the risks. These are:

- The requirement to contract business specialised in emergency server capacity against DDOS attacks;
- The requirement to have a level of malware security deemed adequate by leading security standards;
- The requirement to encourage organisational culture to be actively cyber aware;
- The requirement to periodically re-evaluate employees for signs pre-emptive signs of malevolent intent;
- The requirement to periodically re-evaluate system authorisation of employees.

This answers research question 5: “How can the risks in the design be handled?”.

Chapter 8: Evaluation

8.1 Introduction

This research has presented several findings in response to the research question. This has led to the creation of two artefacts which together form the contribution of this research. These two artefacts are a risk evaluation of the digital identity system regulations and recommendations on addressing the different vulnerabilities. These two contributions can be used to improve the Dutch national requirements set for the digital identity system.

However, before this research concludes with these contributions, it needs to be assessed whether they are actually deemed useful. For this, an evaluation assessment using the Unified Theory of Adoption and Use of Technology (UTAUT) method is used [40]. This evaluation method indicates how well organisations will accept a new technological addition by consulting experts.

This UTAUT method works by presenting the research to a participating expert and then having him/her fill in a questionary on their opinion of the contribution. Based on these responses, it is possible to assess which criteria seem favourable for accepting the contribution and which ones are not.

This chapter first describes the UTAUT method in more detail and how it is adapted for this research. Then, the steps taken for collecting and analysing the data are described. These steps are followed by an overview of the responses made by the participants and a discussion of these results. Lastly, this chapter discusses some limitations before finishing this chapter.

8.2 The UTAUT Method

The UTAUT method is used to evaluate how well technology will be received by its users. This is done by asking experts or other practitioners about their perceptions of the results and recommendations. It is assumed that these participants are carefully selected so that they can give a clear idea of the general attitude of the target audience, which in this case is the Dutch government.

The UTAUT method evaluates a set of propositions based on four main criteria: Performance Expectancy, Effort Expectancy, Social Influence, and Facilitating Conditions. For each of these criteria, the opinion of experts is used to evaluate them. This is done by asking the experts questions on the criteria. The answers to these questions indicate how well the contribution to this research will be accepted. To evaluate the propositions concerning the four main criteria, the experts use their perceptions of the object being evaluated and rate the propositions on a Likert scale ranging from "strongly agree" to "strongly disagree".

The UTUAT style evaluation has been adjusted for this evaluation as not all standard questions have been found to apply. For example, questions related to how it makes an employee’s work easier are not relevant for this research. After all, the focus of this research is cyber resilience and should not affect making work easier for the employee. Therefore, an adaption of the standard UTUAT questions has been made, found in Table 33.

The questions in Table 33 have been asked to the participants of the UTAUT style evaluation. Before the participants were given these questions, they were given a 20 minutes presentation on the topic and the contributions. After this presentation, they were asked to fill in these questions.

Table 33: UTAUT questions

Performance Expectancy (PE)	
Q1	*In my opinion, the results would be useful for the system*
Q2	*In my opinion, using the results increases the cyber resilience*
Effort Expectancy (EE)	
Q3	*To me the implications of the results for the system would be clear and understandable*
Q4	*I think that it is presumable that the benefit of acting on these results would be worth the effort.*
Q5	*In my opinion, efforts to change based on these results would not be disproportionate for the expected scale of the project.*
Q6	*In my opinion, acting on these results would not severely increase the efforts necessary for future changes.*
Social Influence (SI)	
Q7	*I think that the government would support changes based on these results*
Q8	*I think that stakeholders of this system would support changes based on these results*
Q9	*I think that policy makers would support changes based on these results*
Facilitating Conditions (FC)	
Q10	*I think that the government has the knowledge to use these results*
Q11	*I think that the government has the resources to use these results*

8.3 Evaluation research design

8.3.1 Participants.

The UTAUT style evaluation is performed by requesting the professional opinion of participating experts. These experts have been picked because they cover different fields of expertise, which could give a more accurate perspective on the questions. Table 34 describes the qualifications that the experts have that reviewed the usability of the contribution.

Table 34: Expert Roles and Qualifications

Expert	Role in Evaluation	Qualification Description	Years of Experience
1	Government Projects Expert	Senior System Architect at Thales	25+
2	Academical Perspective Expert	Assistant Professor at the University of Twente of the DMB/DS (Data Management & Bionics/Data Science) group.	10
3	Cyber Risk Expert	Senior Cyber Risk Consultant at Deloitte	4
4	Cyber Impact Expert	Assistant Professor at the University of Twente of the IEBIS (Industrial Engineering and Business Information Systems) group.	5

8.3.2. Evaluation Process

The data for the evaluation is obtained in the form of answers to the question form, as seen in Table 33. For these, experts were contacted and were requested to become participants in this evaluation. From these, four experts expressed their intention to participate in this review. These experts were informed that the review entails watching a 20-25 minutes presentation and afterwards filling in a 5 minutes questionnaire. While performing the presentations live would give more information on the reviews, it is harder to arrange a meeting to give the presentation. Therefore, to not burden the participants too much and, as a result, improve the respondent rate, the participants were given the option to watch a recording of the presentation instead.

After receiving the responses to the questionary, the results are analysed. This is done by looking at the lowest, average, and median responses to each of the questions. Based on these, it is possible to tell whether the participants agree with a statement and how much the participants agree with each other. When there is a large discrepancy between these three values, it implies that the participants do not agree with the statement.

8.4 Results & Discussion

From the participants of the UTAUT evaluation method, the summarised results are presented in Table 35. For the ratings, the different possible ratings are labelled from 1 (Strongly Disagree) to 5 (Strongly Agree). The average (Avg.) is calculated by adding all the values of the respondents together and dividing it by the number of participants. The median (Med.) has been given by ordering the respondents' ratings from low to high and taking the middle value.

Table 35: Demographic UTAUT responses

Criteria (N=3)	**Min. (N=3)**	**Med. (N=3)**	**Avg. (N=3)**
Performance Expectancy			
In my opinion, the results would be useful for the system	4	4.5	4.5
In my opinion, using the results increases the cyber resilience	4	4	4
Effort Expectancy			
To me the implications of the results for the system would be clear and understandable	3	4.5	4.25
I think that it is presumable that the benefit of acting on these results would be worth the effort.	4	4	4
In my opinion, efforts to change based on these results would not be disproportionate for the expected scale of the project.	3	4	4
In my opinion, acting on these results would not severely increase the efforts necessary for future changes.	3	3.5	3.5
Social Influence			
I think that the government would support changes based on these results	3	3	3.25
I think that stakeholders of this system would support changes based on these results	3	4	3.75
I think that policymakers would support changes based on these results	3	3.5	3.75
Facilitating Conditions			
I think that the government has the knowledge to use these results	2	2.5	3
I think that the government has the resources to use these results	1	4	3.5

From the results, several criteria require additional discussion for it to come into its own. As such, the different categories will be discussed. While discussing the general response to each category, the questions that provide additional insights will be discussed as well.

The performance expectation questions show that the participants agree that the results would have a favourable performance for the system. Especially because the participants seem to have a common opinion on this, it is presumed that the performance of the contribution will not pose much of an issue with regards to their acceptance.

According to the participants, the effort that is expected to use the contribution of this research seems to be quite reasonable. However, the participants do not seem to agree much on if it will be disproportionate to the scale of the project. While the lowest evaluation is still only neutral, there is a discourse in opinion between the participants. This could be because the participants find it hard to estimate, giving a more conservative answer. In any case, the effort does not seem to be problematic for the acceptance of the contribution. After all, if only taken the worst possible rating, it is still neutral.

When looking at the responses on social influence, it seems that it is trending to a quite neutral response. It is not that the respondents agree or disagree, but it seems that the participants do not necessarily have a strong opinion on the statements. While this could indicate that there is no relation between the contribution and any social influence, this is doubtful as participants have commented on the relation between the wider public and the system. As such, it is more likely that estimating the social influence of requirements is hard due to the abstraction levels. This explains why most of the responses are neutral.

From the facilitating conditions, it can be seen that while the participants consider the government to possess the resources to use the risk assessment and risk treatment recommendations; The participants seem split in whether the government has the knowledge for it. This is a surprising result as the government has access to large knowledge centres that aid its projects. Therefore, it might be strange that the government does not have the knowledge to use these results at first sight. However, there is some sense as to why this could be the case. Namely, the government itself is still in the process of creating its own requirements set. As such, it could be said that as their requirements set is still not finished, they do not have their own knowledge of their own requirements set. This means that when confronted with this contribution, they would lack the knowledge of their own requirements and are therefore unable to use the contribution of this research.

An important observation can be made for the last question, on the resources that the government has to use the results. While most of the experts agreed or strongly agreed, one of the experts strongly disagreed. This expert argued that upon first glance the government might seem to have access to the resources, it does not mean that the government would draw on these resources. This expert argued specifically on the recommendation for emergency server capacity that while these services are available, these are often performed by American firms. As such, European member states would be reluctant to sign contracts for storing data with them, leaving only very few European firms that provide services.

While this only argues about the first recommendation, this could have impact on other recommendations. However, it is to be expected that once governments state their intent to look for firms willing to provide these services, market forces will come into play and ensure that firms will be created to answer these requests.

In any case, it seems that the facilitating conditions could therefore be an issue in the acceptance of the research method. However, as the government is currently investigating what they would want from this field of research, it is likely that they will have this knowledge in the near future. As such, in time, this should not pose a problem.

8.5 Threats to the validity

With the UTAUT style evaluation having been concluded, it is important to look at the threats to the validity of this evaluation. There are three aspects that could affect the validity. These are that the number of participating experts is low and that there is a potential bias for positive results.

The number of participating experts in this evaluation is low. Only four experts were found willing to participate in this evaluation. As such, it could form a potential threat to the validity as it means that these could be the statistical outliers amongst the experts.

However, this seems to be unlikely. The experts as described are all senior experts within their respective expertise and have undoubtedly acquired a feeling for which proposals are likely to be accepted and which are not. This is supported by the notion of Wieringa, who claims that large numbers of experts are not needed to gain substantive answers [39]. According to him, experts who have similar expertise will react similarly to new innovations. As such, it can be derived from this that even if more experts are brought in, they will react similarly. Therefore, while having more respondents would benefit the validity, it is not that much of a threat that the number of experts is low.

The second threat to the validity is a possible bias towards positive answers. The questions that have been created are adaptions of the UTAUT style questions. It is assumed that the original UTAUT style questions had little to no bias, as it is an often-used research method and therefore unlikely to be biased. For the changes made to these questions, the differences are as small as changing the object of the sentence. Therefore, it is assumed that the adaption has not caused an additional bias.

However, there is the risk that having the questions makes it hard not to tailor the material that is evaluated towards them. The evaluation risks becoming biased as the questions could become a checklist for the presentation. This, of course, would mean that the responses to it would be boosted, distorting the validity of the evaluation.

Therefore, the presentation was created before the full list of questions was prepared. As such, it is presumed that the question list had no influence on the presentation. As such, the risk of conformity bias towards positive answers is mitigated as much as possible.

Therefore, while there exist threats to the validity of this evaluation, it is assumable that these have not impacted the evaluation on a significant level. As such, there is confidence that the results represent the usability of the risk assessment and the risk treatment recommendations. If future works tries to improve upon this usability, Appendix E gives an evaluation on which adjustments to the methods can be considered.

8.6 Conclusion

In conclusion, to evaluate the method that this thesis contributed, a UTAUT-based evaluation was performed. This evaluation showed that the contribution scored well on *expected performance* and *effort expectancy*; it was unclear how well the *social influence* would be. Furthermore, while the participants agreed that the government would have the resources to implement the contribution, there was a split in whether the government had the knowledge to use the contribution of this research. In general, however, the facilitating conditions for this contribution seemed to be positive.

Therefore, the answer to RQ6 is that the contribution of this research seems to be deemed very useful by experts in the field. As such, it has a good chance of being accepted by the Dutch government once they have created an initial national requirement set.

Chapter 9: Discussion

9.1 Introduction

The empirical evaluation of the newly proposed method has been performed, and the core findings have been discussed in detail in the previous chapter.
In this chapter, a reflection on the whole research process is provided. The reflection starts with discussing the topic, the research method, and the findings. Then we continue with a discussion on the implications for practice and for research. Finally, we reflect on the limitations of this research.

9.2 Discussion on the Scope of Research

9.2.1 Diverse perspectives on the topic are hindering the definition of the scope

As the research on Digital Identity in E-Commerce progressed over the months, insight has been gained into what this entails. In the experience of the author of this thesis, the subject turns out to be much more multi-faceted than it initially seemed. Research in this area appears to be prone to distribution to other disciplines, with the risk of the project becoming unmanageable in size. This is because one can look in many different ways at the project and possibly justify a number of relevant theoretical perspectives. If looked at from a financial point of view, this will lead to financial viability requirements. When a consumer point of view is taken, it leads to usability requirements. In order to prevent this master's thesis from becoming unmanageable in size and therefore illegible, restrictions have been placed on the subject. This is discussed in more detail later in this chapter.

The spread of publications on the subject of this master thesis to other scientific disciplines tends to occur because so few comparative materials exist. This makes defining the topic difficult. If there were more sources on the subject, not every aspect would have to be explored, as it would be sufficient to refer to an existing source. This would help stay on the subject without getting side-tracked too much.

It is the expectation of the author, that in the future, more sources will be available on identity in E-commerce and implementations of EU regulation 2015/1502. This will be all the more the case when the actual national requirements of the Netherlands have been made available. However, until this moment, the problem of having a very multi-faceted topic will likely continue.

9.2.2 Decisions depend on national agendas of the EU member states

In this study, it is found that there is a great deal of dependence on decisions made by national governments. Although the EU has created a framework with its regulations, it is left up to the Member States to create an implementation that fits the framework. There is, however, no obligation for the Member States to carry out this implementation. Without any obligation for EU member states to start implementing the proposed digital identity system, it is unlikely that the governments will publish new documentation of the system.

The urgency for implementing the EU regulation may be lacking in the eyes of the national governments. Up until the moment of finishing up this thesis, little attention has been paid to this regulation. Other projects may have large public support or influential lobbyists supporting them. For example, projects related to environmental sustainability have significant public and lobbyists backing them. The people who would decide on budget distribution would be reluctant to fund a project with little attention when there are projects with much attention. The result of this is that nations will be reluctant to invest in creating this project.

Furthermore, we can safely assume that the EU member states might become more interested in investing in their own project if they have a successful example. Furthermore, having a successful example is likely to attract public support to create similar systems in other EU member states. This would make it more likely that similar projects in other EU member states will receive funding.

Furthermore, having a successful example would make the process of creating similar systems easier. After all, they can rely on documentation of this example and learn from the lessons learned. This would be especially important for EU member states that are not as familiar with large scale digital projects. EU member states such as Albania and Lithuania would especially benefit from this as they have neither the expertise nor the funding to create such large scale projects without example. As such, it is likely that after the first EU member state has implemented the system, which is most likely the Netherlands, the other EU member states will be quick to follow. This will increase the number of sources significantly.

However, the Netherlands has decided to be the first EU member state attempting to create this system. This means that they will not benefit from the advantage of having examples. The Netherlands does, however, gain some benefit from being an early adapter. Amongst the benefits is that the Dutch government can shape the system to their liking and make it fit perfectly with their national requirements. Other EU member states that are later to adapt will have to adapt their system to be compatible with the Dutch system, limiting their ability to fit their own national requirements. This can be a significant advantage for nations that want to build additional infrastructure, as it becomes easier to fit those ambitions. For example, the Netherlands might want to expand the infrastructure to better cooperate with the logistical operations in the port of Rotterdam. This would make tracking illegal transports much easier.

9.3 Discussion on research methods

This study used various methods to answer the main research question and the associated research questions. When investigating suitable methods to answer these research questions, the problem of abstraction levels often played a role. A notable example is the use of high-level requirements (which means being specified at a high abstraction level). This was also noted by the experts involved in evaluating the study, as evidenced by their assessments.

It is not uncommon for research to address an issue by looking at the issue from various levels of abstraction. An example of this practice is examining employee compliance with guidelines, where guidelines are still very abstract and the employee practice is already more concrete. Usually, this does not create issues as transitions between these levels of abstraction will be made understandable with concrete evidence. This helps provide both the reader and the researcher with anchor points that are understandable and prove the correctness of the transition. However, since there has been no previous research in this area with any concrete results, most transitions had to be supported by abstract evidence. For example, transitioning from requirements to vulnerabilities is not supported by having an actual system. Rather, this is only supported by creating an Archimate model of the system, requiring more interpretation when following the transition. This makes every transition more difficult to follow.

This can be solved by carrying out more research into concrete implementations of the EU requirements. The advice to do more research has been repeated throughout this thesis, but it is the most important bottleneck. The scale of this field is immense, with hardly any research relatable to it. This makes researching in this field very difficult.

Last but not least, before starting the reflection on the use of research methods, the author of this thesis sought external feedback by senior cybersecurity researchers at the University of Twente, on the set up of the research process. For this purpose, the author asked these researchers to use the evaluation criteria for scientific research that are used in their scientific conferences. This external feedback is added in Appendix E. The author of the thesis reflected on the research methods in light of the feedback and together with his supervisors, a decision was made to set up an evaluation study based on the UTAUT model [40] in order to assess the usefulness of the contributions of the thesis to experts in the field.

9.4 Discussion on Implications of the Results

In this thesis, the results are presented to answer the six research questions. These results have already been discussed in the discussion of the chapters in which the results were presented. Therefore, the discussion in this section focuses on the implications of the results.

9.4.1 Implication for Practice

The main implication that this research has provided for practice is that *the cyber resilience of the EU requirements is insufficient for direct implementation*. The present research supports this statement by using assessments of the vulnerabilities and examples of how these can be exploited. We think that this implication is important for the Dutch government as they should evaluate these EU requirements before they are implemented and adapt them if necessary. Our study helps with this by providing a list of recommended additional requirements. Both the indication that the cyber resilience is insufficient and the list of recommended additional requirements are readily available to assist the Dutch government in its decision-making. Because the Dutch government is currently solely responsible for transforming EU requirements into Netherlands-specific requirements, the Dutch requirements are the only requirements to be discussed in the context of this study. Therefore, the government officials are the major actor for whom there are practical implications.

Finally, it is the understanding of the author that other countries' governments can possibly benefit from the results and the implications of this study. Although they do not fall within the scope of this study, they can still assess whether their contextual settings correspond to those of the Dutch government. According to the research methodologist R.Wieringa [39], similar organisations are expected to have similar reactions when confronted with new systems used in very similar contexts. Therefore, it is expected that once the Dutch government has created a system, other governments might well be inclined to accept the same system if they share the same interests, level of commitment, values and process-oriented thinking. If this is the case, then this study is likely to have the same implications for them as for the Dutch government.

9.4.2 Implication for Future Research

The findings of this research have several implications for future research. According to the findings, the EU regulations have several glaring vulnerabilities which will need to be addressed. This research focussed on the cyber security of the system, but if weaknesses could be identified, it is possible that by looking at it with a different scope could identify more weaknesses. Focussing on privacy with GPDR or Dutch domestic law would be worthwhile to research. It would also be worthwhile to investigate if it might have consequences for vulnerable groups in society, like refugees and the elderly.

Examples of research questions worthwhile investigating in the future and analysing the system through a different scope would be:

- *How well is the privacy of citizens guaranteed in this system?*
- *Does the system comply with Dutch domestic law?*
- *Will the system have unintentional consequences for vulnerable groups in society?*

Another avenue of future research would be to explore deeper the relationship between requirements and technical architecture as well as the evolution of cybercriminals' methods in light of the adoption of the EU regulations. This would then build directly on our current research. Examples of research questions would then be:

- *How would the requirements of EU Regulation 2015/1502 translate into an architectural model?*
- *How will cybercriminals adapt their methods to an implementation of EU Regulation 2015/1502?*

Translating the EU regulation 2015/1502 into an architectural model would make the regulation more concrete, and it would help the individual EU member states develop their own country-specific architectural model. This could improve the quality and speed of the national development projects. As part of this research, national differences should be taken into account. For example, the Netherlands has already embraced digital identity, while in Germany, this is not yet the case. Therefore, an analysis of the national discussions on digital identity should be performed. Based on this, appropriate models can be created for the proposed digital identity system.

Predicting how cybercriminals would alter their methods in response to the proposed identity system, would help protect against this migration of crime. For this, criminology has developed prediction models for migrating criminals [46]. By using these models, it would be possible to predict how various groups of criminals, based on their characteristics, will redistribute themselves amongst the various current criminal activities. For example, criminals who commit low-tech crimes in e-commerce will not be able to move to high-tech crime but would migrate to other low-tech crimes. This prediction can be validated with a quantitative analysis of criminal prosecutions. Based on what other areas e-commerce criminals are currently engaged, it is possible to predict where they are likely to migrate towards when the proposed digital identity system is implemented. Based on this research, recommendations can be made for new preventive policies.

Answering either of the proposed future research questions that build on top of this research would help in predicting the way the e-commerce field will evolve further. This will contribute by both making the system more concrete and assisting in the development of the system itself. While doing this, it would be highly advised to consult governmental sources as new information is expected to be published between this study (November 2021) and the start of future works.

9.4.3 Implications for future education

This research discusses the cyber resilience as reflected in the regulations for a European digital identity system for E-commerce. From this research, implications can be drawn for the education, in particular for the teachers and students involved in E-Commerce courses.

The first implication is that students will need to be prepared for the new addition to the E-commerce infrastructure. After students graduate, most of them will join tech companies as consultants or system designers. When the new addition to the E-commerce infrastructure becomes known to platforms providing E-commerce services, these platforms will need support in adapting to it. Similar to how businesses, both small and large, needed help in implementing GDPR. The students that would graduate by then, will then have to provide consultancy or help design a new system. Educating the students on this upcoming addition to the E-commerce infrastructure would help them in fulfilling this task, thereby preparing them better for the future.

The second implication is about what needs to be addressed in this education. The proposed infrastructure changes by the EU will bring change to how everyone will use e-commerce. This means that business models might need to be adapted. For example, with fraudulent activities of cybercriminals being more likely to be identified and subsequently prosecuted, the number of frauds in E-commerce will drop. Therefore, on could expect that it would become easier to trust potential transaction partners, resulting in more trusted buying and selling options. This significantly changes the viability of business models for businesses relying on being one of the few trusted transaction partners in their niche market.

Furthermore, cybercriminals would also change their behaviour in response to the circumstances that impede their fraudulent activities. They will likely change their methods to avoid being caught, creating new upcoming security threats and revitalising old security threats. Educating the students on how business models might be impacted and how the model of criminals changes would prepare the students better for the future.

The third implication is to continue teaching adherence to basic security principles and to keep in mind the possibility of infrastructure failure. As shown in this research, there are security flaws in the EU regulations which could jeopardise the system itself if not addressed. Therefore, students must continue to be taught that there is no such thing as perfect security. They should be taught the principle of layered defence and contingency planning in the event of security failure. This would best prepare the students for their work or research life.

9.5 ArchiMate Architectural Model for research: an example

9.5.1 Reasons for providing example Architectural models

This research project treats requirements sources and standards that provide directions and guidance and focus on what needs to be considered in regard to identity systems, while having nearly nothing on the "how" aspects (e.g. how this needs to be achieved). In light of this, we lack any concrete requirements that could be translated into architecture design choices. The high-level requirements are open to an extent that they allow for a broad range of possible architectures. However, when attempting to create a possible architecture, one necessarily has to make assumptions – this is because the requirements are too high-level and therefore abstract. We think that making assumptions might be dangerous, as little country-specific regulation-related foundation exists. It would be a lot of guessing regarding the context of a particular country, for example the Netherlands, where very little is known at the present time regarding the choices that the Dutch Government to strengthen cyber-resilience. As a high level of abstraction in the sources makes it difficult to come up with a universal reference architecture that follows solid reasoning and justification of the design choices, we think that it is more practical to provide an example of one possible architecture for illustrative purposes. In addition, in section 9.4.2 several directions for further research are given. One of the possible directions proposed is the creation of an architecture reference model. This reference model will graphically illustrate the system, which assists in seeing the big picture of the system and how each part interacts with the other parts. This helps in making the vague requirements more concrete.

On one hand, the example architecture model, as the end product of this thesis, will help others to understand the subject. On the other hand, the existence of example models will help researchers in their research. During this research into cyber resilience, insight was gained into the system. It will be very helpful when this insight is reflected in a first example model when investigating architectural models for the proposed digital identity system.

If no research has yet been done on possible architectural models, an example model can also be helpful for those investigating different aspects of the proposed digital identity system.

9.5.2 Assumptions for the ArchiMate model

Before one can make an architectural reference model, several assumptions are necessary. These assumptions are needed because there are various ways to implement the EU regulations. Therefore, while the architectural models of each interpretation will satisfy the requirements, the models will be substantially different from each other. To assist further researchers as much as possible, the assumptions on which these architectural models rely are described. If any of the assumptions are no longer valid or applicable in future research, the example architectural models may not be suitable anymore for system explanation.

For clarity, the assumptions are divided into General Assumptions (GA) and Technical Assumptions (TA). In Table 36 and Table 37, these assumptions are listed. The motivations of these assumptions are described after the tables. The decisions for these assumptions are desktop decisions, but knowing their motivation could assist in understanding what would change if an assumption is no longer applicable.

Table 36: General Assumptions of an example architecture

#	General Assumption (GA)
1	*The EU member states have not published their architecture which can serve as an example.*
2	*The entire architecture is designed without taking into account phasing the system.*
3	*Financial and political requirements play no role in the system design.*
4	*All parts of the system should have a meaningful role in achieving the task of the system.*
5	*The architecture is not built as an extension of an already existing institution.*

The first assumption is that no EU member states have created and published their country's specific reference architecture (GA-1) yet. This assumption is made because if a government creates their architectural model, it becomes an example for other EU member states developing their models later. Other EU member states might create their country's specific systems in resemblance to the first governmental architecture. After all, it is a safe choice to adopt a proven architecture, only making minor adjustments to fix the mistakes in the architecture. Therefore, based on the first architecture made and its success, the eventual architectural models of other EU member states will essentially correspond to the original reference model.

The second assumption (GA-2) is the assumption that there is no phasing in the system implementation. A phased implementation may depend on many factors. For example, it could rely on the expectancy of a government concerning milestones. The size of an implementation team, the budget, or the project risk assessment can also influence the phasing. Due to the wide range of factors that influence the phasing, different models/systems will eventually form the implementation outcome. After all, phasing is only possible if the system's architecture allows it to be phased along pre-determined lines. Therefore, many system variants should be given as an example, especially in regard to the many variables that influence phasing decisions. Therefore, to increase clarity and universality, it will be assumed that phasing is not relevant to the architectural model.

For similar reasons, financial and political requirements are assumed to play no role in system design (GA-3). We acknowledge that financial and political conditions differ from state to state, making it difficult to account for. Since it is assumed that states will imitate or copy the identity system example, it makes sense that financial and political circumstances cannot play a role.

The fourth general assumption states that the reference system components must play a meaningful role in performing the system's tasks (GA-4). The primary task is to match e-commerce account owners to their real identities. So only those things that are directly related to the primary tasks are taken into account when building the reference model. Example-architecture models may include other elements for other tasks of a system, such as tracking e-commerce statistics for national institutions. It wouldn't be very wise to include these tasks in a sample architecture. Therefore, only elements with a performance target of the primary or secondary tasks of the system are considered.

Lastly, the assumption that the architecture should not be part of an already existing system (GA-5). With this assumption, the focus will lie on creating **a new system**. If the system were to be a part of another existing system, it would mean that it would have to be adapted to that previous architecture. Such integration between systems would only make the architecture more complex and harder to follow.

Table 37: Technical Assumptions of an example architecture

#	Technical Assumption (TA)
1	*Except for the verification of identity performed by the authority organisations, none of the activities is outsourced.*
2	*The system is organised with as few decentralised elements as feasible.*
3	*All information is end-to-end encrypted.*

The first technical assumption is that only identity verification is outsourced in the architecture (TA-1). This assumption is made because outsourcing is a clear political decision. Some states might be more reluctant than others to do this. Furthermore, outsourcing an activity entails a different architecture, it replaces an internal activity with external communication elements. It is relatively easier to approve an architecture with an activity outsourced as you only have to define the requirements for the outsourced activity. Nevertheless, we assume an architecture with only the authority organisation' activity outsourced.

The second technical assumption is that the system operates as centralised as possible (TA-2). Although decentralising does reduce the impact of some risks, it also introduces complexity in the system. Furthermore, at the same time, it could present a higher probability of cyber-security incidents. The EU regulation does not prescribe a decentralised system, but the opposite is also not specified. Therefore, to both reduce complexity and improve comprehensibility, the system will be centralised as far as feasible.

Finally, the assumption is that all information is end-to-end encrypted (TA-3). This assumption is made mainly to reduce the clutter in the architectural models. Without this assumption, every time information flows, it would require encryption and decryption. As a result, the models will be more complex, and it would be harder to read and understand the models. By adding this assumption, the encryption and decryption do not necessarily have to be displayed in the architectural models. Thereby it reduces the clutter and improves understandability.

9.5.3 Example Architectural Models

With the assumptions as stated in 9.5.2, an example of a reference architecture has been made using the ArchiMate conventions. Again, as already indicated earlier, this is by no means the only architecture that can be made under these assumptions but provides for a clear and understandable example. This can guide further research into creating a validated architectural framework for the proposed e-commerce identity system.

This architecture is viewed from six different viewpoints. These will explain different parts of the system and put them in a different light. These viewpoints can be found in Table 38, along with their intended purpose.

Table 38: Example Architecture Viewpoints

Viewpoint	Purpose
Organisation	It shows the different departments of the system.
Actor Co-operation	It shows how and what information flows between the departments of the system.
Information Structure	It shows what user's information is involved in this system.
Infrastructure Usage	It shows how the technological elements are connected to each other and to the application elements.
Application Usage	It shows how the application elements are connected to each other and to the business elements.
Business Process Co-operation	It shows how the business processes are connected to each other and to the application elements.

An explanation is given underneath the image for each viewpoint to interpret correctly and to understand the viewpoints.

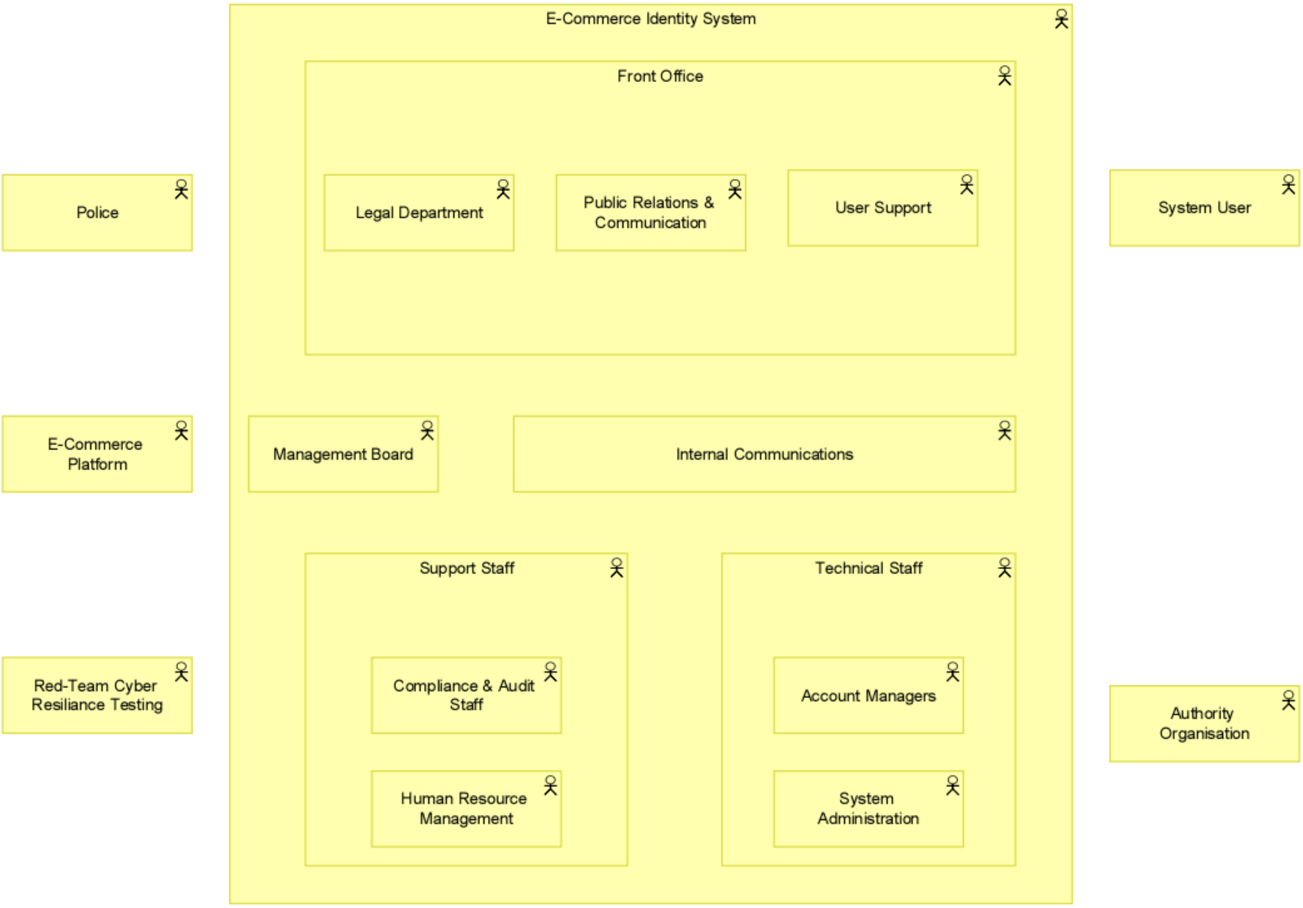


Figure 21: Organisational Viewpoint

In Figure 21, an organisation viewpoint is provided of the proposed digital identity system. As can be seen in this figure, it contains the management board, internal communications, support staff, technical staff, and the front office. In addition, while actually not part of the organisation, the five actors relevant to the system are displayed. This is because this same viewpoint is expanded upon in the actor co-operation viewpoint. These have been added in their respective places to improve understandability to make the overcrowded second viewpoint easier to read. These will be discussed in the next viewpoint.

The technical staff has been divided up into two departments: the account managers and the system administrators. While their names give a good indication of their roles and purposes, the necessity of splitting these up might not be clear at first sight. Their skillsets could be quite overlapping.

The reason for still creating these two departments is to prevent their activities from competing with each other. At the same time, it is reasonable to place two groups of similar skillsets together to have a larger team capable of handling more requests. However, it could risk one of their activities taking up all their time, leaving no time for other critical activities. For example, if massive numbers of account requests are being processed, a combined group would not have time to work on the system itself anymore. This could result in a backlog of a particular type of activity without anyone noticing. After all, the number of delayed activities might be low compared to the number of processed activities, avoiding it being noticed based on statistics. In order to prevent this from happening, the two groups are separated based on their essential activity.

In the support staff, there are two departments: the compliance & audit staff and the human resource management. These two departments speak mostly for themselves. The only thing noteworthy is specifying what is expected that the compliance & audit staff does. As shown in Figure 21, there is actually an actor, the red-team cyber resilience testers, who would help in the testing of the system. As such, the compliance & audit staff would focus on internal auditing and the processing of intelligence they would get from the external audits.

The front office is divided into: the legal department, public relations & communications, and user support. The legal department would focus on any legal questions that would arise from within the organisation and from outside. These would most likely often entail requests for information from the police. After all, every request of theirs for the identity of an account owner would have to be reviewed. These would be most appropriate to be done by the legal department, as this would fall within their skillset. Based on their review, they could refuse to provide account details or provide the requested information.

Public relations & communication deals with keeping the public up to date and communicating with the actors involved with the system. This department should be given enough room to determine its best course of action. After all, the best way to reach a target audience might change over time. For example, ten years ago, newsletters were the predominant way to inform the public, while currently, this is done with social media.

Then the last department of the front office is user support. As trust of the system users is very important for the system's future, it is important that the system users are sufficiently supported in their use of the system. As such, there should be a dedicated department for helping the service users with their requests.

In-between the other departments is the management board, which makes the decisions for the system itself. This is not part of any other department as these will be making decisions for the entire system. When future research is done into creating an architectural framework for the system, it could be a worthwhile avenue to research what roles and responsibilities need to be fulfilled in this management board. Based on this, a proposed management board composition can be made.

Lastly, the choice for an internal communications department has been made. This department would facilitate communications between the various departments. While an architecture can be made without this department by letting the different departments send their information directly, this has some drawbacks. The most important being that this would open up the possibility of files getting lost, which could happen for various reasons. For example, email lists not having been updated, there being no designated person with responsibility, or pending requests without replying. This department could resolve these issues by keeping itself up to date with all of the human resource changes and keeping track of open requests. This would ensure that the system would not fall prey to a lack of information governance.

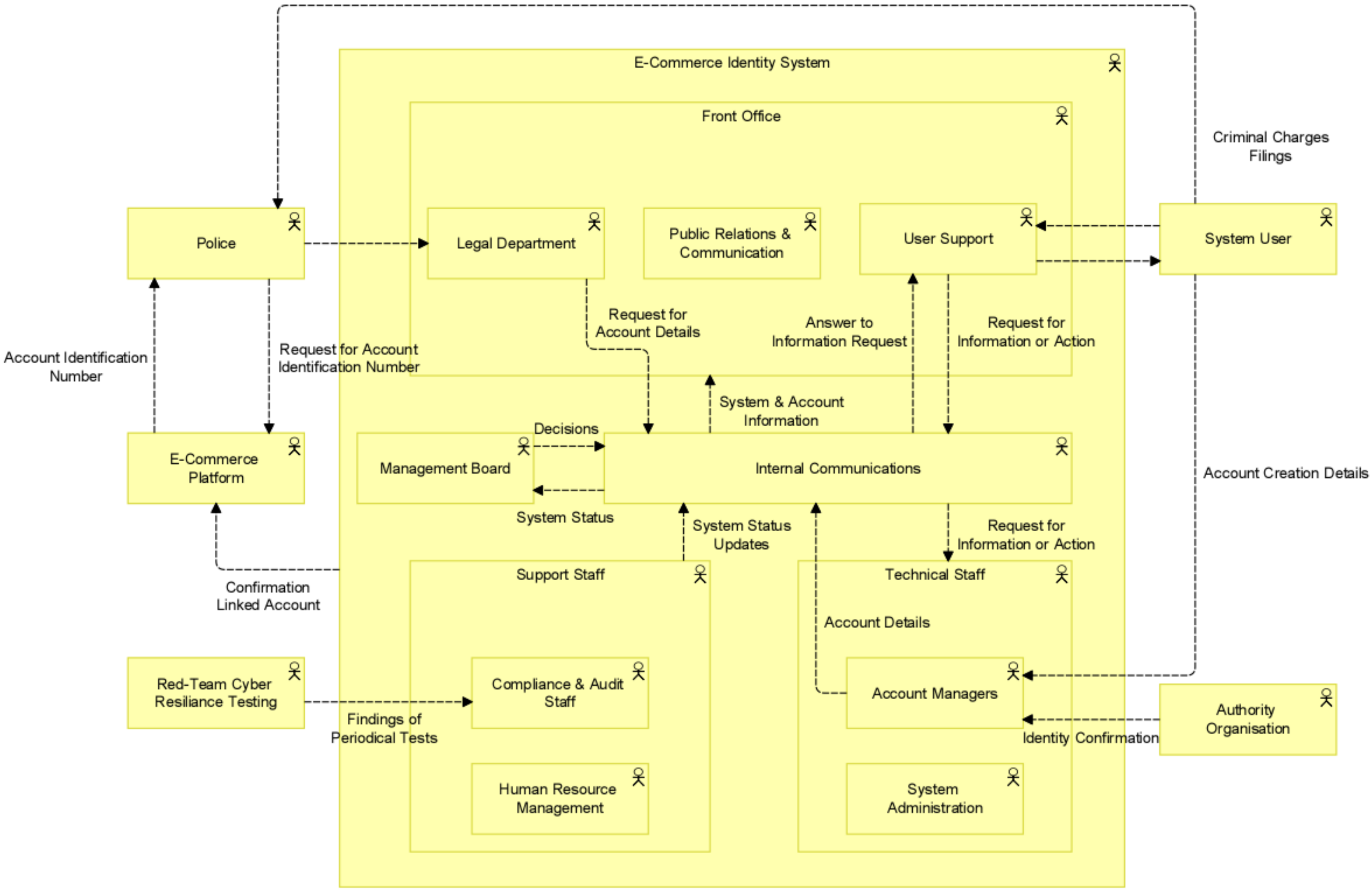

E-Commerce Identity System
Front Office
Criminal Charges Filings
Police
Legal Department
Public Relations & Communication
User Support
System User
Account Identification Number
Request for Account Identification Number
Request for Account Details
Answer to Information Request
Request for Information or Action
System & Account Information
Decisions
E-Commerce Platform
Management Board
Internal Communications
Account Creation Details
System Status
System Status Updates
Request for Information or Action
Confirmation Linked Account
Support Staff
Technical Staff
Account Details
Red-Team Cyber Resiliance Testing
Compliance & Audit Staff
Account Managers
Authority Organisation
Findings of Periodical Tests
Identity Confirmation
Human Resource Management
System Administration

Figure 22: Actor Co-operation Viewpoint

As found in Figure 22, the actor co-operation viewpoint shows how the different actors involved with the proposed digital identity system exchange information. As explained in the organisational viewpoint, a decision has been made to route the internal communications through a specialised department. This receives all of the internal communications and redirects them to their appropriate actors. In this viewpoint, only the often reoccurring information flows have been shown. After all, including all possible incidental communications would create clutter, taking away the model's clarity. When future research defines an appropriate reference framework, it might help to create an inventory of all the incidental communications that would be necessary.

Another information flow that would need to be expanded upon is the public relations & communications department, as seen in Figure 22. In this current figure, it seems as if this has no information flows at all. While in reality, it is more likely that it has information flows to all external actors. However, this would not contribute enough to justify adding additional clutter mainly because it would mean that many additional external actors would have to be added to the framework. These actors are, For example, businesses, the Dutch parliament, European Commission, and European Data Protection Supervisor (EDDS). Keeping these actors informed would be the task of this department, meaning that an architectural model should be created on this.

As already introduced in the organisational viewpoint, the actor co-operation viewpoint considers five external actors that are part of the information flow. These are e-commerce platforms, authority organisations, system users, the police, and red team cyber resilience testers. These actors have their information flows to and from the system clearly explained through the text surrounding the relations.

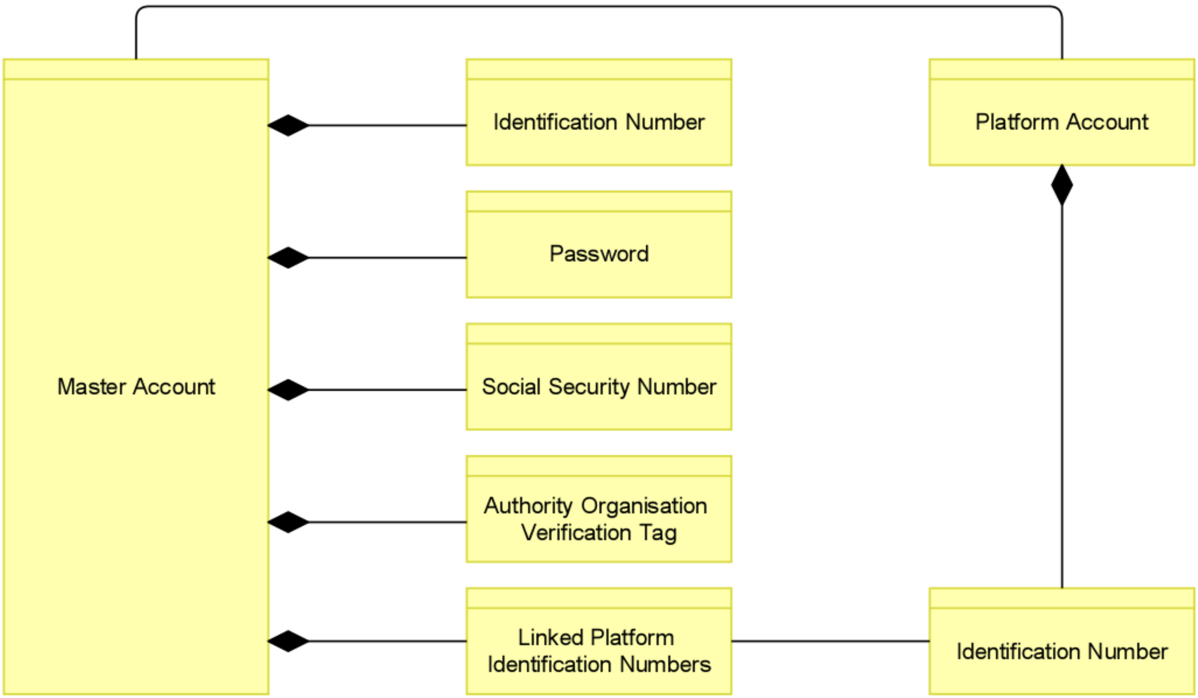


Figure 23: Information Structure Viewpoint

In the Information Structure Viewpoint, as shown in Figure 23, the type of information stored is presented. As shown, the Master account, stored in the system itself, comprises five types of data. Whereas, the platform accounts, which are stored not in the system itself but on the e-commerce platforms, only have a single data type.

The idea behind this is that when an account has acted maliciously on an e-commerce platform, the identification number can be retrieved from the platform's database. This identification number has been listed under a master account in the proposed digital identity system. By searching for the identification number of the platform account in all the master accounts, it is possible to trace the account owner. After all, the master account has a social security number that the government can trace back in their own systems.

A tag of the authority organisation is added to counter the threat of authority organisations going rogue and handing out verifications without verifying the identity. This helps in two ways. First, if many frauds seem to have the same verification tag, it might be possible that this authority organisation has been too loose in its verification methods. Therefore, this authority organisation might require its compliance checked. Secondly, in the case of an authority organisation going rogue, it would help block the falsely made accounts. Without it, it becomes hard to figure out those accounts which were authorised by the authority organisation and, therefore, might need re-evaluation.

A desktop decision has been made to have a list of platform identification numbers attached to the master account. This serves the purpose of tracking down the frauds and blocking their accounts. However, there is a different architecture possible that could perform the same service. For example, by having the platform account keep a record of which master account is linked to it. This would take away the need to have an identification number for the platform account.

Storing data on the e-commerce platforms would have as an advantage that it would reduce the data stored in the system self, and instead store it decentral. In the case of the system getting hacked, this would prevent hackers from knowing where someone has e-commerce platform accounts. This will limit the possibility of it being abused in identity theft.

However, decentralising data does increase another risk. After all, it would give e-commerce platforms a tag for users that is the same on all other platforms. This would mean that after some e-commerce platforms have suffered from data leaks, which is more likely as these platforms are more plentiful and do not necessarily have good security, a list of these tags would be available. Based on this, it would be easy for e-commerce platforms to figure out for themselves who the owner of an account is based on these leaks in combination with other information like delivery addresses. This would give the e-commerce platforms the ability to falsely create platform accounts using the master account identification number and then frame it for fraud.

Especially in the case of high-profile civilians like prime ministers or other politicians, this poses a severe risk. This risk can easily be avoided by keeping the unique master account identification numbers in the system and keeping the record of where the owner of the master account has platform accounts also in the system. This prevents malicious e-commerce platforms from creating fake accounts in order to frame someone.

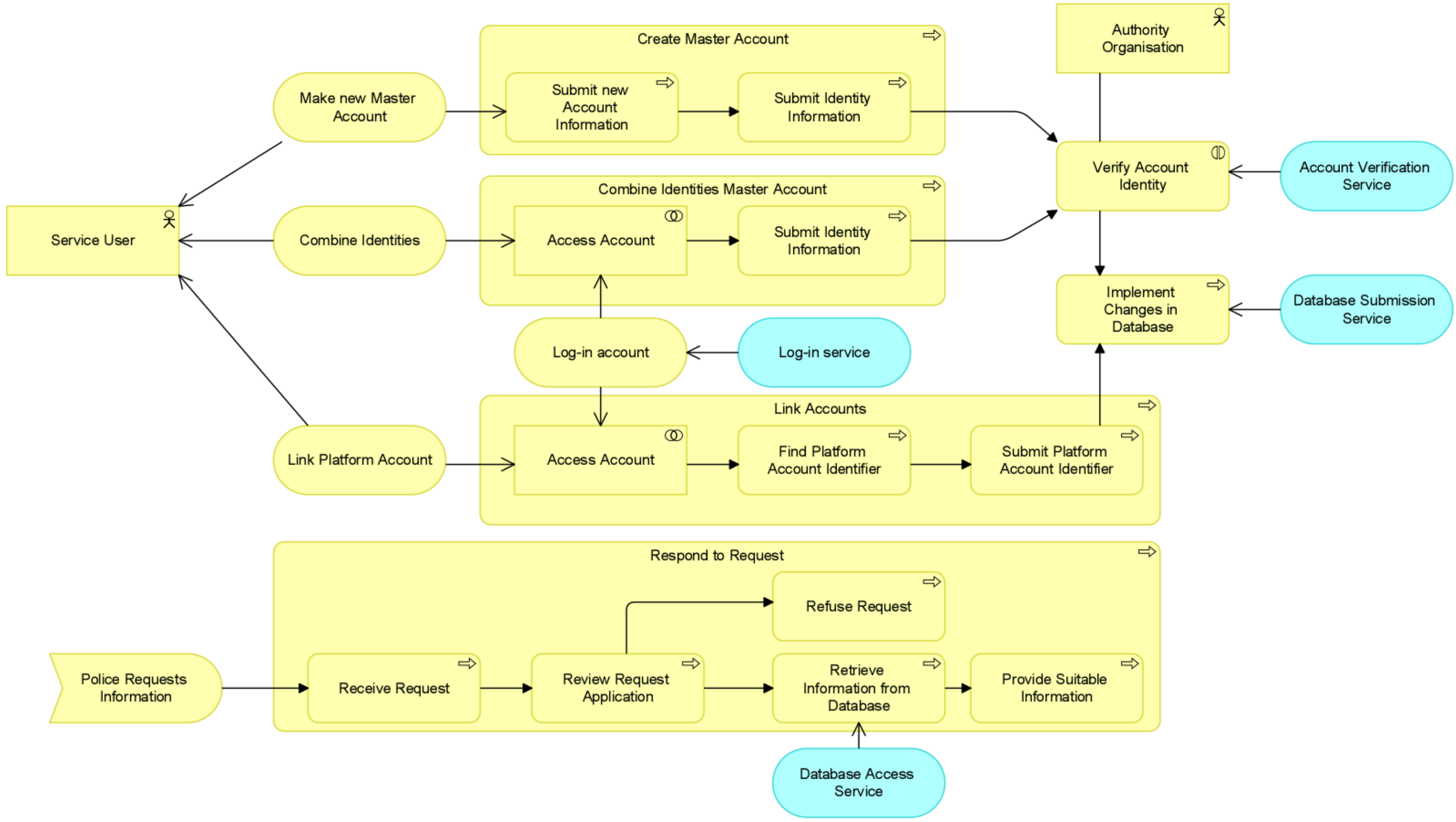

Create Master Account
Make new Master Account
Submit new Account Information
Submit Identity Information
Authority Organisation
Verify Account Identity
Account Verification Service
Service User
Combine Identities Master Account
Combine Identities
Access Account
Submit Identity Information
Implement Changes in Database
Database Submission Service
Log-in account
Log-in service
Link Accounts
Link Platform Account
Access Account
Find Platform Account Identifier
Submit Platform Account Identifier
Respond to Request
Refuse Request
Police Requests Information
Receive Request
Review Request Application
Retrieve Information from Database
Provide Suitable Information
Database Access Service

Figure 24: Business Process Co-operation Viewpoint

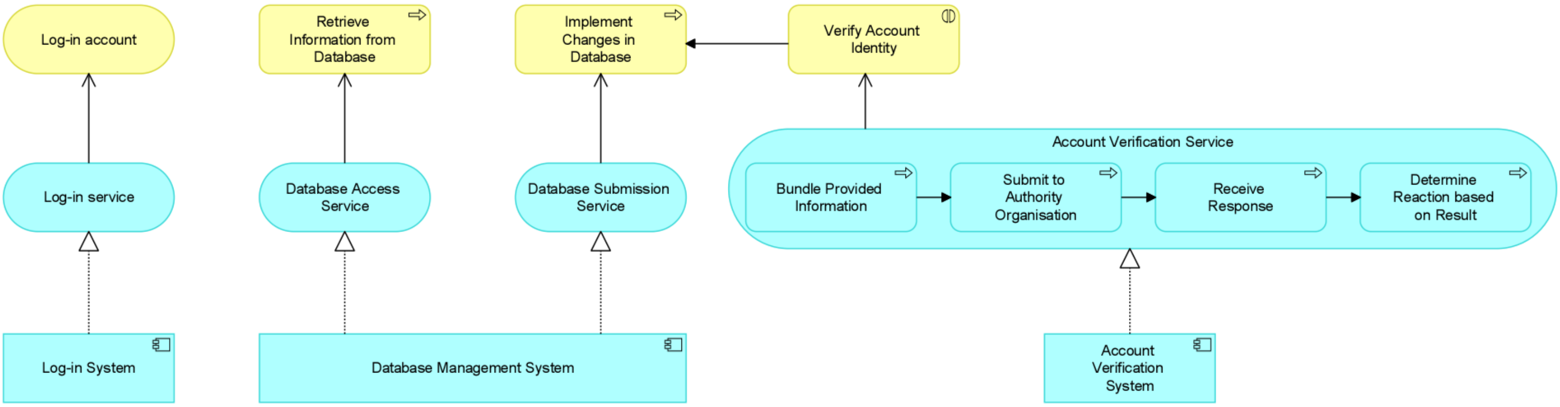

Log-in account
Retrieve Information from Database
Implement Changes in Database
Verify Account Identity
Log-in service
Database Access Service
Database Submission Service
Account Verification Service
Bundle Provided Information
Submit to Authority Organisation
Receive Response
Determine Reaction based on Result
Log-in System
Database Management System
Account Verification System

Figure 25: Application Usage Viewpoint

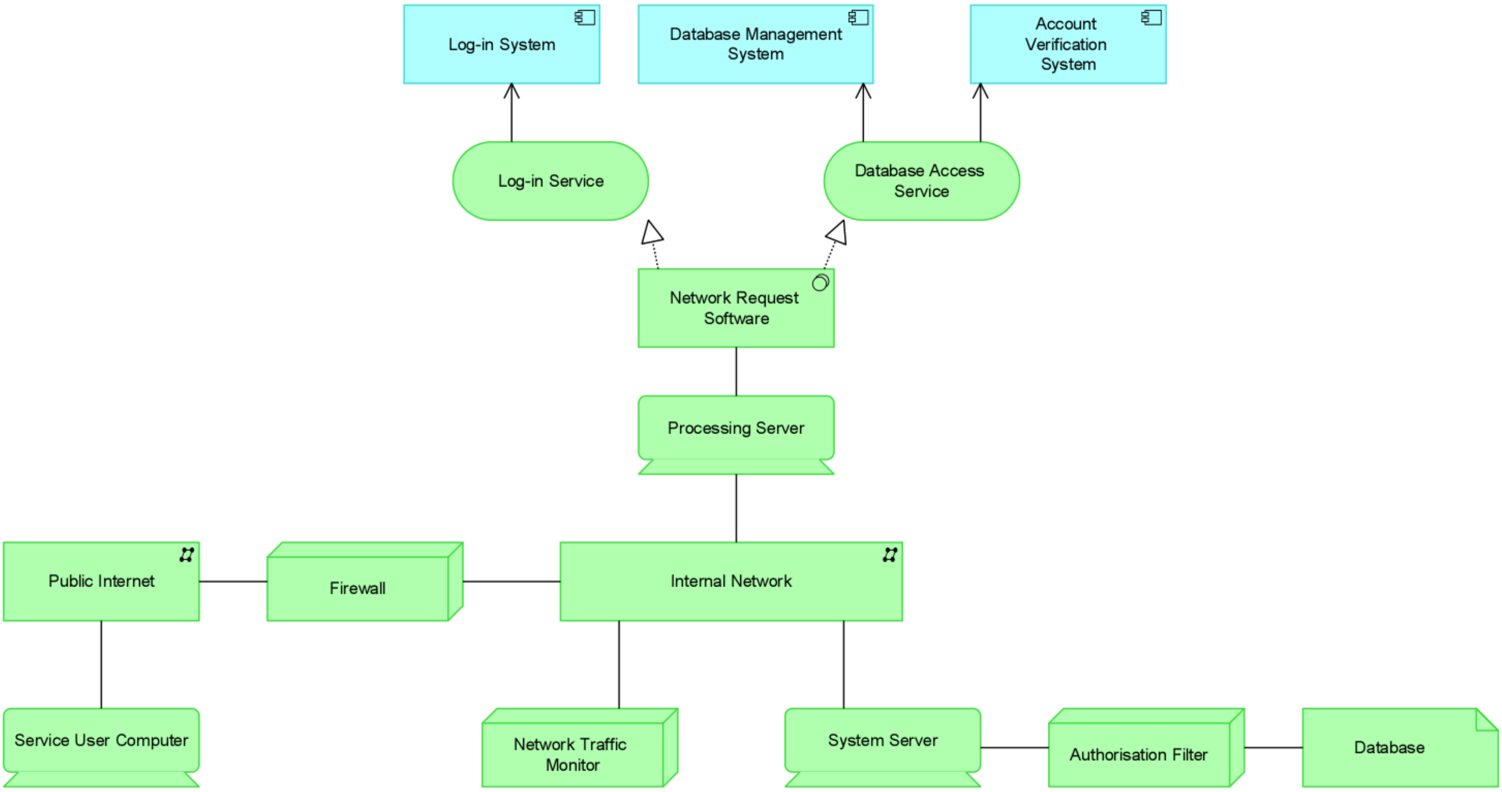


Figure 26: Infrastructure Usage Viewpoint

In Figure 24, the Business Process Co-operation Viewpoint is shown. This explains how the business process interacts with each other and with the application layer. As the proposed identity system will likely have a hundred or so business processes, the design choice has been made to focus solely on the business processes related to the primary tasks of the system. This resulted in four main business processes that are explained.

As shown in Figure 24, some of the business architecture is used by multiple business processes. For example, the business process of validating the identity is used multiple times as it is used to create an account and add additional identities to the account. The latter is, for example, important when the owner of the master account has his own business. Then this person might want to add the legal identity of this business to the account.

As a suggestion for future research into the architectural model, it would be wise to create categories of business processes. As the system will encompass many business processes, it would create a confusing architecture if these are all displayed in one big viewpoint. Therefore, categorisation seems to be the most optimal solution. The categorisation of business processes is quite a worthwhile endeavour and could, therefore, even become a sub-research question of that research.

As presented in Figure 25, the Application Usage Viewpoint shows how the business processes connect to the application layer. In contrast to the business process co-operation viewpoint, the focus of this viewpoint is on the application layer. However, as shown in Figure 25, this layer does not have many components at the moment. This is not because the proposed digital identity system does not use applications at all. In contrast, it is more likely that a lot of internal applications are used. However, it would not make sense for the essential standard business processes to be distributed across several different systems. After all, this would mean that the one performing the business process has to switch between applications constantly. This would be not very enjoyable to do. Therefore, the decision has been made to limit the number of times someone has to switch applications. However, this should not be overdone either. As each time applications are fused, they reduce the flexibility and of the application. This might mean that eventually, the application itself becomes incredibly hard to use. Therefore, a middle ground needs to be sought between having a different application for each business process and limiting the number of applications necessary to perform sequential business processes. This has been done in the Application Usage Viewpoint.

In the last viewpoint on infrastructure usage, the infrastructure attached to the application components is shown in Figure 26. This infrastructure is based around a central internal network to which all the servers are connected. This will allow the different servers to exchange information and route the traffic coming from the public internet. However, in-between this internal network and the public internet, a firewall has been placed. This will provide the first layer of security.

The second layer of security is in the monitoring of the network traffic in the internal network. This layer is very important as the firewall only protects against threats from outside the network, meaning that it will not do much against internal threats. Therefore, this network traffic is monitored to find signs of an infection.

Lastly, there is an authorisation filter in-between the system servers and the database. This is to prevent access to the account files for those that should not have access. These can be fine-tuned to fit the actual usage of the system. Nevertheless, it is suggested that a restrictive approach should be taken. After all, the database itself will contain a large dataset of private data. Apart from the users accessing their own data, only upon request of the police should the employees themselves look into the database. It should be limited to only that data related to the account in question when this is done. Furthermore, access must be for a limited time. This would best ensure that employees would find no way of misusing the system to obtain private data.

The system could be organised way differently in the infrastructure as well. For example, currently, the methods of the internal network are not specified. This could be a bus network topology, a point-to-point, or a tree network if just a few possibilities are named. This could be greatly expanded and would result in very different models.

In summary, the above architectural framework is one of the many forms that the system could possibly take. The framework is intended, among other things, as a reference model to gain a first insight into the system, especially for those who will research this area.

9.6 Limitations

As mentioned in the previous chapter, this research has some limitations. These are not only by the design of this research, as pointed out in chapter 1, but some have formed over the course of this research. This section will focus on the latter.

The most notable limitation is that this study has the most relevance when EU member states have not yet created their own country-specific systems. This is because this study focuses on the development of the systems. Once the systems have been created for all EU member states, it can still have relevance in indicating possible flaws in its implementations, as there is the risk that the members states will not have addressed them.

Secondly, the requirements of the EU regulation are very high-level (and therefore one can consider them abstract). This makes their comprehension troublesome for those not familiar with them. For example, the author witnesses that high-level requirements make it difficult for those reviewing this research to fully understand the outcomes of this thesis, despite their relevant expertise. The abstraction level makes it easier to lose track of a train of thought. The research would have benefitted from more concrete EU regulations in order to address the topic. Having more concrete requirements would also make the research more understandable for those with less expertise in either e-commerce or cyber security.

Thirdly, a limitation of this work is that not all different possible perspectives have been covered. For example, the aspect of privacy has not yet been fully explored in this study. Likewise, issues like an increased effort to provide proof of one's innocence have not been explored either. Both the privacy and the innocence issue would already be worth investigating on their own.

Fourthly, this research has used a single method for identifying the vulnerabilities. While it is to be expected that the most glaring vulnerabilities have been identified, there could be vulnerabilities that have been missed. These could be vulnerabilities that are only discovered when using a method specialised for them. As such, it is advised that future research could use other methods in order to ensure that no blind spot has formed as a result of using a single method of vulnerability identification.

Finally, in the UTUAT style evaluation, only four experts evaluated the results. Although at first glance, it might be seen as a major issue, it is, in fact, not as much of an issue and more of a limitation. According to the research-methodological source of Wieringa [39], experts in the same field, who tend to work on similar projects, will react similarly to the acceptancy of a system. As a result, it is to be expected that including additional similar experts would not result in drastically different results. Therefore, one might assume that only by finding radically different experts would give new insights. However, it is then questionable if those new insights actually reflect the acceptance by the Dutch government. As such, it is more a limiting factor that the number of reviewers is low.

Chapter 10: Conclusion

10.1 Research Questions

This research questioned if the requirements provided by the EU for an international digital identity system for E-Commerce is sufficient to protect against cyber-attacks. It has formulated the following main research question to address this:

"Are the currently proposed requirements for an international Digital Identity system for E-Commerce sufficient to reasonably protect the interests of stakeholders against cyber-attacks?"

In order to address this main research question, it is divided into five sub research questions. These five questions contributed to answering this main research question by performing the steps of the ISO 31000:2018 standard for risk management.

RQ1. *Which stakeholder interests are relevant for the system design?*

The first research question establishes what should be protected. This is done by performing a stakeholder analysis. Although there are many stakeholders and different drivers, it has been found that the different drivers can be reduced to four categories. These categories are Trust, Private Data, Economic Continuity, and Economic contribution.

RQ2. *What technical requirements are imposed upon the system design?*

The second research question goes further by establishing the context of the research topic, for example, by looking at how the protection of the interests of stakeholders is currently envisioned. To this end, a systematic literature review was conducted on both legal sources and academic sources. The result of this has been a set of mechanisms which can be found in Table 7. In addition, these mechanisms have been supplemented with information on how digital identity can be established, for which a graphical representation can be found in Figure 12.

RQ3. *What vulnerabilities could arise from the proposed requirements?*

Combining the results of the first two research questions makes it possible to apply vulnerability identification techniques. The technique used is the unified killchain method. This method has provided insight into the potential vulnerabilities in the requirements of the system. These vulnerabilities are: Insufficient server capacity, Insufficient protection against malware, Malicious actions by an employee in disguise, Access of employees to internal systems, and Assumed trustworthiness of Authority organisations.

RQ4. *What risks arise from the vulnerabilities in the requirements?*

With the vulnerabilities identified in research question 3, risks are identified with cyber threat analysis. This showed that the greatest risk is posed by insufficient protection against malware. The risks posed by the vulnerabilities in order of gravity are:

- Very High Risk
  - The level of malware defence is not specified
- High Risk
  - Absent requirements related to the server capacity of the system
  - Absent controls against employees performing malicious activities
  - Absent requirements for retracting unnecessary network access of employees
- Low Risk
  - Re-evaluation of authority organisations is not specified

RQ5. *How can the risks in the design be handled?*

As additional contributions to this topic, appropriate measures have been identified as well. This was done according to the ISO 31000:2018 method. As a result, five additional requirements have been devised, which could be added to the national set of requirements as possible responses to the risks. These five additional requirements are:

- Requirement to contract companies that specialise in emergency server capacity against DDOS attacks;
- Requirement to have a level of malware protection considered adequate by leading security standards;
- Requirement to encourage organisational culture to be actively cyber aware;
- Requirement to periodically re-evaluate employees for signs of malevolent intent;
- Requirement to periodically re-evaluate the system authorisations of employees.

RQ6. *What is the proposed artefact's usefulness perceived by experts in the field?*

Using a UTAUT style evaluation, this research has evaluated the usefulness of the risk assessment (RQ4) and the risk treatment recommendations (RQ5). This evaluation showed that they scored well on the criteria *expected performance* and *effort expectancy*; it was unclear how well the *social influence* would be. The experts had varying opinions for the facilitating requirements, doubting whether the Dutch government had the knowledge available for this project already. In conclusion, it seemed that most of the criteria did point towards good usability, according to the experts.

Looking back at the main research question, whether the currently proposed requirements are sufficient, it is clear from the sub research questions that the requirements are not sufficient. Therefore, additional measures are needed to protect the targeted system against cyber-attacks reasonably. In the next section, the main findings and recommendations of this research will be presented.

10.2 Key Findings and Recommendations

In this study, the following results were found, and the following recommendations were made. In order to improve the clarity, the findings are in italics, and the recommendations are placed below the findings.

1. *The cyber resilience of the EU requirements is insufficient*

The main research question of this study was whether the EU requirements would be sufficient to protect the interests of stakeholders against cyber-attacks. This study has shown that this is not the case. Several major shortcomings have been identified in the requirements. While some were expected to be acceptable, most risks need to be addressed before any implementation is built. Failure to do so may lead to the total failure of the project.

2. *Vulnerabilities arise from both missing requirements and vague requirements*

The risks exist because the EU regulation leaves the interpretation of the requirements to the EU Member States. As a result, several requirements are made very vaguely, which could be considered a good thing as it covers as much as possible. However, this has the disadvantage that it becomes easier to state that a system complies with the requirements without detailed specification. This is not necessarily intentional, as it also makes it more difficult to identify what the system is missing without these detailed specified requirements. As such, these types of requirements pose potential vulnerabilities.

However, despite the vague requirements, some requirements seem to be missing. These missing requirements relate specifically to security controls. These requirements can prevent anyone from noticing a security breach.

3. *Cyber resilience needs to be improved by adding new requirements*

In order to address the risks, it is recommended that the Dutch government sets additional requirements to improve the cyber resilience of the final system. Although there are alternative means to improve cyber resilience, these are only recommended as a supplement. After all, the general principle of security by design specifies that it is better to make already plans for defences instead of adding them as a supplement.

The advice for the Dutch government is to go beyond these recommendations by adding additional measures. This will create a defence-in-depth, which is much more reliable than a single layer of defence. Furthermore, these measures will have to be reassessed in case new information might arise.

4. *More Direct sources should be made available*

This brings us to the next point, which is that sources on the subject are currently scarce. Although there are sources that overlap with the subject, there are hardly any sources that address the system. This limits the development of the area, as it requires both practitioners and researchers alike to define and prove everything themselves. This severely hinders the growth of the field.

As such, this study recommends that researchers perform more research in this area. An example of an area expected to be worth exploring concerns the paradox that better identification is detrimental in proving actual innocence. This additional research makes the field more concrete and therefore also more attractive to other researchers. This amplification effect could drag this project out of obscurity while improving the quality of the definitive system.

In order to aid new researchers in becoming familiar with the proposed identity system, an example architecture has been created in section 9.5. This example architecture also provides an initial direction for research into the creation and improvement of the system's architecture.

Appendices

Appendix A: Bibliography

[1] Knops, R.W. (2021). Visiebrief digitale identiteit [Letter of government]. Accessed on 17 May 2021 through: https://www.rijksoverheid.nl/documenten/kamerstukken/2021/02/11/kamerbrief-over-visie-digitale-identiteit

[2] McGrath, S.K. & Whitty, J. (2017). Stakeholder defined. International Journal of managing Projects in Business, 10(4), 721-748.

[3] Oxford Learner's Dictionary. Definition of stakeholder noun from the Oxford Advanced Learner's Dictionary. Accessed on 17 May 2021 through: https://www.oxfordlearnersdictionaries.com/definition/english/stakeholder?q=stakeholder

[4] Mitchell, R.K., Agle, B.R., & Wood, D.J. (1997). Towards a Theory of Stakeholder Identification and Salience: Defining the Principle of Who and What Really Counts. The Academy of Management Review, 22(4), 853-886.

[5] Rowley, J. (2011). e-Government stakeholder-Who are they and what do they want?. International Journal of Information Management, 31(1), 53-62.

[6] Freeman, R.E. (1984). Strategic management: A Stakeholder Approach. Cambridge University Press. DOI: 10.1017/CBO9781139192675.

[7] Kitchenham, B. (2004). Procedures for Performing Systematic Reviews. Accessed on 30 May 2021 through: http://www.inf.ufsc.br/~aldo.vw/kitchenham.pdf

[8] European Parliament, Council of the European Union (2014). Regulation 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. Accessed on 5 June 2021 through: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0910&qid=1623501331415

[9] European Commission (2015). Commission Implementing Regulation 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. Accessed on 5 June 2021 through: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015R1502&qid=1623501358512

[10] Canada, & European Union (2017). Comprehensive Economic and Trade Agreement (CETA) between Canada, of the one part, and the European Union and its Member States, of the other part. Accessed on 5 June 2021 through: https://eur-lex-europa-eu.ezproxy2.utwente.nl/legal-content/EN/TXT/?uri=CELEX%3A22017A0114%2801%29&qid=1622282978689

[11] European Union, & Japan (2021). Agreement between the European Union and Japan for an Economic Partnership. Accessed on 5 June 2021 through: https://eur-lex-europa-eu.ezproxy2.utwente.nl/legal-content/EN/TXT/?uri=CELEX%3A22018A1227%2801%29&qid=1623502567292

[12] European Union, & Singapore (2020). Free trade Agreement between the European Union and the Republic of Singapore. Accessed on 5 June 2021 through: https://eur-lex-europa-eu.ezproxy2.utwente.nl/legal-content/EN/TXT/?uri=CELEX%3A22019A1114%2801%29&qid=1623502720064

[13] CARIFORUM States, & European Union (2017). Economic Partnership Agreement between the CARIFORUM States, of the one part, and the European Community and its Member States, of the other part. Accessed on 5 June 2021 through: https://eur-lex-europa-eu.ezproxy2.utwente.nl/legal-content/EN/TXT/?uri=CELEX%3A22008A1030%2801%29&qid=1623502745512

[14] Merriam-Webster. Natural Person. Accessed on 10 June 2021 through: https://www.merriam-webster.com/legal/natural%20person

[15] Merriam-Webster. Legal Person. Accessed on 10 June 2021 through: https://www.merriam-webster.com/legal/legal%20person

[16] Mocanu, S., Chiriac, A.M., Popa, C., Dobrescu, R., & Saru, D. (2019). Identification and Trust Techniques Compatible with eIDAS Regulation. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST 284, 656-665.

[17] Engelbertz, N., Erinola, N., Herring, D., Somorovsky, J., Mladenov, V., & Schwenk, J. (2018). Security analysis of EIDAS – The cross-country authentication scheme in Europe. 12th UNESENIX Workshop on Offensive Technologies, WOOT 2018.

[18] Tsakalakis, N., O'Hara, K., & Stalla-Bourdillon, S. (2016). Identity Assurance in the UK: Technical implementation and legal implications under the eIDAS Regulation. WebSci 2016 – Proceedings of the 2016 ACM Web Science Conference, 55-65.

[19] Průša, J. (2015). E-identity: Basic building block of e-Government. 2015 IST-Africa Conference, IST-Africa 2015, 7190586.

[20] Cuijpers, C., & Schroers, J. (2014). EIDAS as guideline for the development of a pan European eID framework in FutureID. Lecture Notes in Informatics (LNI), Proceedings – Series of the Gesellschaft fur Informatik (GI), P-237, 23-38.

[21] Graux, H. (2013). Moving towards a comprehensive legal framework for electronic identification as a trust service in the European Union. Journal of International Commercial Law and Technology, 8(2), 110-117.

[22] Sädtler, S. (2013). Identity management in cloud computing in conformity with European Union law? - Problems and approaches pursuant to the proposal for a regulation by the European Commission on electronic identification and trust services for electronic transact. Lecture Notes in Informatics (LNI), Proceedings – Series of the Gesellschaft fur Informatik (GI), P-223, 118-129.

[23] Mitre. Att&CK. Accessed on 5 July 2021 through: https://attack.mitre.org/

[24] Lockheed Martin. The Cyber Killchain. Accessed on 5 July 2021 through: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

[25] Lockheed Martin (2015). Gaining the advantage; Applying cyber killchain methodology to network defense. Accessed on 5 July 2021 through: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

[26] Pols, P., Dominguez, F., & Fox-IT. (2017). The Unified Killchain; Raising resilience against advanced cyber attacks. Accessed on 5 July 2021 through: https://www.unifiedkillchain.com/assets/The-Unified-Kill-Chain.pdf

[27] Pols, P., Burghouwt, P., & Van den Berg, J. (2017). The Unified Killchain; Designing a unified killchain for analyzing, comparing and defending against cyber attacks. Accessed on 5 July 2021 through: https://www.unifiedkillchain.com/assets/The-Unified-Kill-Chain-Thesis.pdf

[28] Statista (2021). E-commerce worldwide statista dossier. Accessed on 10 August 2021 through https://www.statista.com/study/10653/e-commerce-worldwide-statista-dossier/

[29] Ravelin. Online Payment Fraud. Accessed on 10 August 2021 through https://www.ravelin.com/insights/online-payment-fraud

[30] Felson, M., & Clarke, R.V. (1998). Opportunity Makes the Thief. Policing and Reducing Crime Unit.
https://popcenter.asu.edu/sites/default/files/opportunity_makes_the_thief.pdf

[31] ENISA (2019). ENISA Threat Landscape Report 2018; 15 Top Cyberthreats and Trends. Accessed on 30 July through https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018/

[32] Passeri, P. (2021). Q2 2021 Cyber Attack Statistics. Accessed on 30 July 2021 through: https://www.hackmageddon.com/2021/07/22/q2-2021-cyber-attack-statistics/

[33] ISO. ISO 31000:2018(en) Risk management – Guidelines. Accessed on 20 August 2021 through: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

[34] Kasperksy. What is a honeypot. Accessed on 22 August 2021 through: https://www.kaspersky.com/resource-center/threats/what-is-a-honeypot

[35] Mission Critical magazine. The Dark Web DDOS Attacks sell for as low as $10 per hour. Accessed on 24 August through: https://www.missioncriticalmagazine.com/articles/93185-the-dark-web-ddos-attacks-sell-for-as-low-as-10-per-hour

[36] European Business Review. The high price businesses pay in case of a DDOS attack. Accessed on 25 August through: https://www.europeanbusinessreview.com/the-high-price-businesses-pay-in-case-of-a-ddos-attack/#:~:text=Immediate%20Costs,and%20%241.6M%20for%20enterprises.

[37] Lodder, A.R., & Murray, A.D. (2017). Regulation (EU) no 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eidas regulation). Eu regulation of E-commerce: A commentary, 256-289.

[38] Berbecaru, D., Atzeni, A., Benedictis, M.D., & Smiraglia, P. (2017). Towards Stronger Data Security in an eID Management Infrastructure. 25th Euromicro International Conference on Parallel, Distributed and Network-Based Processing, 391-395.

[39] Wieringa, R.J. (2014). Design science methodology for information systems and software engineering. Springer Publishing. DOI: 10.1007/978-3-662-43839-8

[40] Venkatesh, V., Morris, M.G., Davis, G.B., & Davis, F.D. (2003). User Acceptance of Information Technology: Toward a Unified View. MIS Quarterly, 27(3), 425-478.

[41] Verschuren, P., & Doorewaard H. (2010). Designing a Research Project. Eleven International Publishing.

[42] Straight, B. (2021). E-Commerce cybercrime jumped 50% in 2020. Consulted on 2 November 2021 through: https://www.freightwaves.com/news/e-commerce-cybercrime-jumped-50-in-2020

[43] Alexander, I.F., & Beus-Dukic, L. (2009). Discovering Requirements: How to Specify Products and Services.

[44] Lund, M.S., Solhaug, B., & Stølen, K. (2012). Model-Driven Risk Analysis: The CORAS Approach. DOI: 10.1007/978-3-642-12323-8

[45] Fox-IT. (2012). Black Tulip: Report of the investigation into the DigiNotar Certificate Authority breach. DOI: 10.13140/2.1.2456.7364

[46] Waardenburg, L., Sergeeva, A., & Huysman, M. (2018). Digitalizing crime: How the use of predictive policing influences police work practices. 34th EGOS Colloquium, 2018.

Appendix B: Abbreviations

Abbreviation	Unabbreviated
AO	Authority Organisation
C2	Command & Control
DDOS	Distributed Denial Of Service
DMB/DS	Data Management & Bionics/Data Science
EE	Effort Expectancy
eIDAS	Electronic IDentification, Authentication and trust Services
ENISA	European Union Agency for Cybersecurity
EU	European Union
FC	Facilitating Conditions
IEBIS	Industrial Engineering and Business Information Systems
MFN	Most Favourable Nation
PE	Performance Expectancy
RQ	Research Question
SI	Social Influence
SLR	Systematic Literature Review
UTAUT	Unified Theory of Adoption and Use of Technology

Appendix C: Regulation (EU) 2015/1502 Technical specifications and procedures [9]

2.1. *Enrolment*

2.1.1. Application and registration

Assurance level	Elements needed
Low	1.Ensure the applicant is aware of the terms and conditions related to the use of the electronic identification means. 2.Ensure the applicant is aware of recommended security precautions related to the electronic identification means. 3.Collect the relevant identity data required for identity proofing and verification.
Substantial	Same as level low.
High	Same as level low.

2.1.2. Identity proofing and verification (natural person)

Assurance level	Elements needed
Low	1.The person can be assumed to be in possession of evidence recognised by the Member State in which the application for the electronic identity means is being made and representing the claimed identity. 2.The evidence can be assumed to be genuine, or to exist according to an authoritative source and the evidence appears to be valid. 3.It is known by an authoritative source that the claimed identity exists and it may be assumed that the person claiming the identity is one and the same.
Substantial	Level low, plus one of the alternatives listed in points 1 to 4 has to be met: 1.The person has been verified to be in possession of evidence recognised by the Member State in which the application for the electronic identity means is being made and representing the claimed identity and the evidence is checked to determine that it is genuine; or, according to an authoritative source, it is known to exist and relates to a real person and steps have been taken to minimise the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired evidence; or

	2.An identity document is presented during a registration process in the Member State where the document was issued and the document appears to relate to the person presenting it and steps have been taken to minimise the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired documents; or 3.Where procedures used previously by a public or private entity in the same Member State for a purpose other than the issuance of electronic identification means provide for an equivalent assurance to those set out in section 2.1.2 for the assurance level substantial, then the entity responsible for registration need not to repeat those earlier procedures, provided that such equivalent assurance is confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 of the European Parliament and of the Council [1] or by an equivalent body; or 4.Where electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level substantial or high, and taking into account the risks of a change in the person identification data, it is not required to repeat the identity proofing and verification processes. Where the electronic identification means serving as the basis has not been notified, the assurance level substantial or high must be confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body.
High	Requirements of either point 1 or 2 have to be met: 1.Level substantial, plus one of the alternatives listed in points (a) to (c) has to be met: (a)Where the person has been verified to be in possession of photo or biometric identification evidence recognised by the Member State in which the application for the electronic identity means is being made and that evidence represents the claimed identity, the evidence is checked to determine that it is valid according to an authoritative source; and the applicant is identified as the claimed identity through comparison of one or more physical characteristic of the person with an authoritative source; or (b)Where procedures used previously by a public or private entity in the same Member State for a purpose other than the issuance of electronic identification means provide for an equivalent assurance to those set out in section 2.1.2 for the assurance level high, then the entity responsible for registration need not to repeat those earlier procedures, provided that such equivalent assurance is confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body and steps are taken to demonstrate that the results of the earlier procedures remain valid; or

	(c)Where electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level high, and taking into account the risks of a change in the person identification data, it is not required to repeat the identity proofing and verification processes. Where the electronic identification means serving as the basis has not been notified, the assurance level high must be confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body and steps are taken to demonstrate that the results of this previous issuance procedure of a notified electronic identification means remain valid. OR 2.Where the applicant does not present any recognised photo or biometric identification evidence, the very same procedures used at the national level in the Member State of the entity responsible for registration to obtain such recognised photo or biometric identification evidence are applied.

2.1.3. Identity proofing and verification (legal person)

Assurance level	Elements Needed
Low	1.The claimed identity of the legal person is demonstrated on the basis of evidence recognised by the Member State in which the application for the electronic identity means is being made. 2.The evidence appears to be valid and can be assumed to be genuine, or to exist according to an authoritative source, where the inclusion of a legal person in the authoritative source is voluntary and is regulated by an arrangement between the legal person and the authoritative source. 3.The legal person is not known by an authoritative source to be in a status that would prevent it from acting as that legal person.
Substantial	Level low, plus one of the alternatives listed in points 1 to 3 has to be met: 1.The claimed identity of the legal person is demonstrated on the basis of evidence recognised by the Member State in which the application for the electronic identity means is being made, including the legal person's name, legal form, and (if applicable) its registration number and the evidence is checked to determine whether it is genuine, or known to exist according to an authoritative source, where the inclusion of the legal person in the authoritative source is required for the legal person to operate within its sector and steps have been taken to minimise the risk that the legal person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired documents; or 2.Where the procedures used previously by a public or private entity in the same Member State for a purpose other than issuance of electronic identification means provide for an equivalent assurance to those set out in section 2.1.3 for the assurance level substantial, then the entity responsible for registration need not to repeat those

	earlier procedures, provided that such equivalent assurance is confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body; or 3.Where electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level substantial or high, it is not required to repeat the identity proofing and verification processes. Where the electronic identification means serving as the basis has not been notified, the assurance level substantial or high must be confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body.
High	Level substantial, plus one of the alternatives listed in points 1 to 3 has to be met: 1.The claimed identity of the legal person is demonstrated on the basis of evidence recognised by the Member State in which the application for the electronic identity means is being made, including the legal person's name, legal form, and at least one unique identifier representing the legal person used in a national context and the evidence is checked to determine that it is valid according to an authoritative source; or 2.Where the procedures used previously by a public or private entity in the same Member State for a purpose other than issuance of electronic identification means provide for an equivalent assurance to those set out in section 2.1.3 for the assurance level high, then the entity responsible for registration need not to repeat those earlier procedures, provided that such equivalent assurance is confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body and steps are taken to demonstrate that the results of this previous procedure remain valid; or 3.Where electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level high, it is not required to repeat the identity proofing and verification processes. Where the electronic identification means serving as the basis has not been notified, the assurance level high must be confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body and steps are taken to demonstrate that the results of this previous issuance procedure of a notified electronic identification means remain valid.

2.1.4. Binding between the electronic identification means of natural and legal persons

Where applicable, for binding between the electronic identification means of a natural person and the electronic identification means of a legal person ('binding') the following conditions apply:

(1)It shall be possible to suspend and/or revoke a binding. The life-cycle of a binding (e.g. activation, suspension, renewal, revocation) shall be administered according to nationally recognised procedures.

(2)The natural person whose electronic identification means is bound to the electronic identification means of the legal person may delegate the exercise of the binding to another natural person on the basis of nationally recognised procedures. However, the delegating natural person shall remain accountable.

(3)Binding shall be done in the following manner:

Assurance level	Elements Needed
Low	1.The identity proofing of the natural person acting on behalf of the legal person is verified as having been performed at level low or above. 2.The binding has been established on the basis of nationally recognised procedures. 3.The natural person is not known by an authoritative source to be in a status that would prevent that person from acting on behalf of the legal person.
Substantial	Point 3 of level low, plus: 1.The identity proofing of the natural person acting on behalf of the legal person is verified as having been performed at level substantial or high. 2.The binding has been established on the basis of nationally recognised procedures, which resulted in the registration of the binding in an authoritative source. 3.The binding has been verified on the basis of information from an authoritative source.
High	Point 3 of level low and point 2 of level substantial, plus: 1.The identity proofing of the natural person acting on behalf of the legal person is verified as having been performed at level high. 2.The binding has been verified on the basis of a unique identifier representing the legal person used in the national context; and on the basis of information uniquely representing the natural person from an authoritative source.

2.2. *Electronic identification means management*

2.2.1. Electronic identification means characteristics and design

Assurance level	Elements needed
Low	1.The electronic identification means utilises at least one authentication factor. 2.The electronic identification means is designed so that the issuer takes reasonable steps to check that it is used only under the control or possession of the person to whom it belongs.
Substantial	1.The electronic identification means utilises at least two authentication factors from different categories. 2.The electronic identification means is designed so that it can be assumed to be used only if under the control or possession of the person to whom it belongs.
High	Level substantial, plus: 1.The electronic identification means protects against duplication and tampering as well as against attackers with high attack potential

	2.The electronic identification means is designed so that it can be reliably protected by the person to whom it belongs against use by others.

2.2.2. Issuance, delivery and activation

Assurance level	Elements needed
Low	After issuance, the electronic identification means is delivered via a mechanism by which it can be assumed to reach only the intended person.
Substantial	After issuance, the electronic identification means is delivered via a mechanism by which it can be assumed that it is delivered only into the possession of the person to whom it belongs.
High	The activation process verifies that the electronic identification means was delivered only into the possession of the person to whom it belongs.

2.2.3. Suspension, revocation and reactivation

Assurance level	Elements needed
Low	1.It is possible to suspend and/or revoke an electronic identification means in a timely and effective manner. 2.The existence of measures taken to prevent unauthorised suspension, revocation and/or reactivation. 3.Reactivation shall take place only if the same assurance requirements as established before the suspension or revocation continue to be met.
Substantial	Same as level low.
High	Same as level low.

2.2.4. Renewal and replacement

Assurance level	Elements needed
Low	Taking into account the risks of a change in the person identification data, renewal or replacement needs to meet the same assurance requirements as initial identity proofing and verification or is based on a valid electronic identification means of the same, or higher, assurance level.
Substantial	Same as level low.
High	Level low, plus: Where renewal or replacement is based on a valid electronic identification means, the identity data is verified with an authoritative source.

2.3. *Authentication*

This section focuses on the threats associated with the use of the authentication mechanism and lists the requirements for each assurance level. In this section controls shall be understood to be commensurate to the risks at the given level.

2.3.1. Authentication mechanism

The following table sets out the requirements per assurance level with respect to the authentication mechanism, through which the natural or legal person uses the electronic identification means to confirm its identity to a relying party.

Assurance level	Elements needed
Low	1.The release of person identification data is preceded by reliable verification of the electronic identification means and its validity. 2.Where person identification data is stored as part of the authentication mechanism, that information is secured in order to protect against loss and against compromise, including analysis offline. 3.The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with enhanced-basic attack potential can subvert the authentication mechanisms.
Substantial	Level low, plus: 1.The release of person identification data is preceded by reliable verification of the electronic identification means and its validity through a dynamic authentication. 2.The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with moderate attack potential can subvert the authentication mechanisms.
High	Level substantial, plus: The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with high attack potential can subvert the authentication mechanisms.

2.4. *Management and organisation*

All participants providing a service related to electronic identification in a cross-border context (‘providers’) shall have in place documented information security management practices, policies, approaches to risk management, and other recognised controls so as to provide assurance to the appropriate governance bodies for electronic identification schemes in the respective Member States that effective practices are in place. Throughout section 2.4, all requirements/elements shall be understood as commensurate to the risks at the given level.

2.4.1. General provisions

Assurance level	Elements needed
Low	1.Providers delivering any operational service covered by this Regulation are a public authority or a legal entity recognised as such by national law of a Member State, with an established organisation and fully operational in all parts relevant for the provision of the services.

	2.Providers comply with any legal requirements incumbent on them in connection with operation and delivery of the service, including the types of information that may be sought, how identity proofing is conducted, what information may be retained and for how long. 3.Providers are able to demonstrate their ability to assume the risk of liability for damages, as well as their having sufficient financial resources for continued operations and providing of the services. 4.Providers are responsible for the fulfilment of any of the commitments outsourced to another entity, and compliance with the scheme policy, as if the providers themselves had performed the duties. 5.Electronic identification schemes not constituted by national law shall have in place an effective termination plan. Such a plan shall include orderly discontinuations of service or continuation by another provider, the way in which relevant authorities and end users are informed, as well as details on how records are to be protected, retained and destroyed in compliance with the scheme policy.
Substantial	Same as level low.
High	Same as level low.

2.4.2. Published notices and user information

Assurance level	Elements needed
Low	1.The existence of a published service definition that includes all applicable terms, conditions, and fees, including any limitations of its usage. The service definition shall include a privacy policy. 2.Appropriate policy and procedures are to be put in place in order to ensure that users of the service are informed in a timely and reliable fashion of any changes to the service definition and to any applicable terms, conditions, and privacy policy for the specified service. 3.Appropriate policies and procedures are to be put in place that provide for full and correct responses to requests for information.
Substantial	Same as level low.
High	Same as level low.

2.4.3. Information security management

Assurance level	Elements needed
Low	There is an effective information security management system for the management and control of information security risks.
Substantial	Level low, plus: The information security management system adheres to proven standards or principles for the management and control of information security risks.

High	Same as level substantial.

2.4.4. Record keeping

Assurance level	Elements needed
Low	1.Record and maintain relevant information using an effective record-management system, taking into account applicable legislation and good practice in relation to data protection and data retention. 2.Retain, as far as it is permitted by national law or other national administrative arrangement, and protect records for as long as they are required for the purpose of auditing and investigation of security breaches, and retention, after which the records shall be securely destroyed.
Substantial	Same as level low.
High	Same as level low.

2.4.5. Facilities and staff

The following table represents the requirements with respect to facilities and staff and subcontractors, if applicable, who undertake duties covered by this Regulation. Compliance with each of the requirements shall be proportionate to the level of risk associated with the assurance level provided.

Assurance level	Elements needed
Low	1.The existence of procedures that ensure that staff and subcontractors are sufficiently trained, qualified and experienced in the skills needed to execute the roles they fulfil. 2.The existence of sufficient staff and subcontractors to adequately operate and resource the service according to its policies and procedures. 3.Facilities used for providing the service are continuously monitored for, and protect against, damage caused by environmental events, unauthorised access and other factors that may impact the security of the service. 4.Facilities used for providing the service ensure that access to areas holding or processing personal, cryptographic or other sensitive information is limited to authorised staff or subcontractors.
Substantial	Same as level low.
High	Same as level low.

2.4.6. Technical controls

Assurance level	Elements needed
Low	1.The existence of proportionate technical controls to manage the risks posed to the security of the services, protecting the confidentiality, integrity and availability of the information processed.

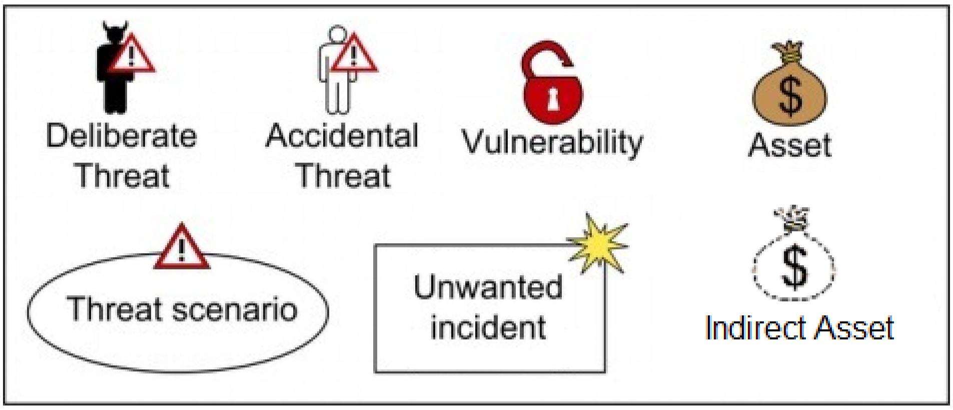
	2.Electronic communication channels used to exchange personal or sensitive information are protected against eavesdropping, manipulation and replay. 3.Access to sensitive cryptographic material, if used for issuing electronic identification means and authentication, is restricted to the roles and applications strictly requiring access. It shall be ensured that such material is never persistently stored in plain text. 4.Procedures exist to ensure that security is maintained over time and that there is an ability to respond to changes in risk levels, incidents and security breaches. 5.All media containing personal, cryptographic or other sensitive information are stored, transported and disposed of in a safe and secure manner.
Substantial	Same as level low, plus: Sensitive cryptographic material, if used for issuing electronic identification means and authentication is protected from tampering
High	Same as level substantial.

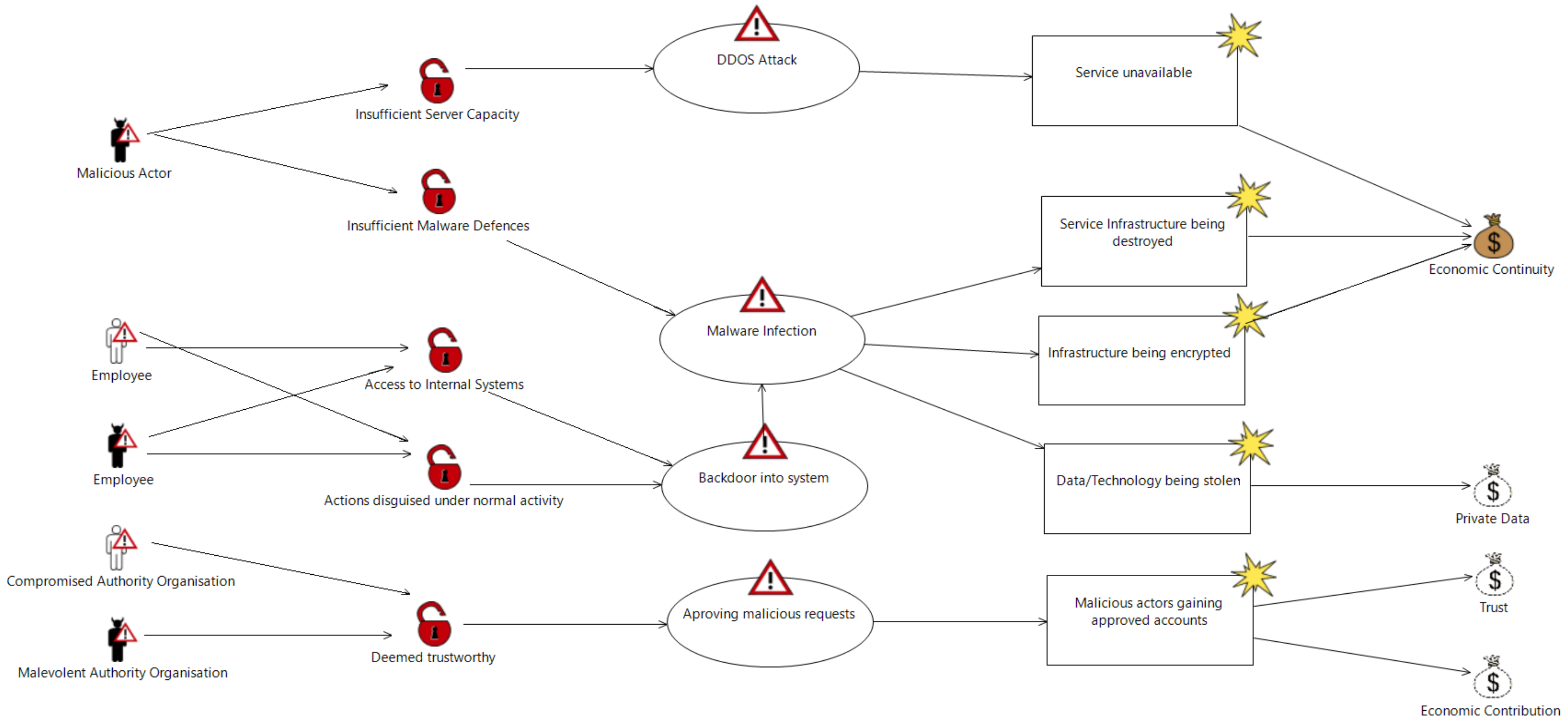
2.4.7. Compliance and audit

Assurance level	Elements needed
Low	The existence of periodical internal audits scoped to include all parts relevant to the supply of the provided services to ensure compliance with relevant policy.
Substantial	The existence of periodical independent internal or external audits scoped to include all parts relevant to the supply of the provided services to ensure compliance with relevant policy.
High	1.The existence of periodical independent external audits scoped to include all parts relevant to the supply of the provided services to ensure compliance with relevant policy. 2.Where a scheme is directly managed by a government body, it is audited in accordance with the national law.

[1] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30).

Appendix D: Vulnerability Findings in CORAS




Malicious Actor
Insufficient Server Capacity
Insufficient Malware Defences
DDOS Attack
Service unavailable
Economic Continuity
Employee
Access to Internal Systems
Employee
Actions disguised under normal activity
Malware Infection
Backdoor into system
Service Infrastructure being destroyed
Infrastructure being encrypted
Data/Technology being stolen
Private Data
Compromised Authority Organisation
Malevolent Authority Organisation
Deemed trustworthy
Aproving malicious requests
Malicious actors gaining approved accounts
Trust
Economic Contribution

Appendix E: Validation

E.1 Introduction

This chapter presents the validation phase of the research study. Due to the abstract nature of this research, it is not feasible to perform any kind of practice tests as a form of validation. In this study, several levels of abstraction are involved. Validation methods are available for the different individual levels, but they are not applicable for multiple levels. That is why validation by means of expert reviews was chosen for this study, as this method does not have this limitation. This is done by providing the participating experts with the results from this study so far combined with the questions to give feedback and their opinion on the validity. This procedure corresponds to the peer review method that is followed when publishing scientific articles in journals.

This chapter describes the validation by means of expert reviews. First, the method is described in more detail and then how the method is used for the validation in this research. Subsequently, the results from this validation are presented and analysed.

E.2 Method

E.2.1 Method Set-Up

As explained, the validation will be done through expert review. This corresponds to the peer review method, which is also applied for scientific articles in journals. The idea behind this method is that experts in a certain field can estimate how trustworthy research is due to their experience in the field. Since this method is based on the validation method for scientific journals, it makes sense to consult academic experts. While it is possible to consult industry or government experts, they are less suited for scientific validation but more for practical validation.

It is not feasible to have this research validated by government experts because the commission, which has to find out what the government wants, is still in the preliminary phase at the time of this research. So the experts should come from the academic and business sector.

Although practical validity is also important, the question is to what extent this can be measured. The reviewers are experts in their field and are regularly hired by companies or governments. As a result, their comments in assessing the study will also reflect the practical validity.

The method is carried out by giving the review participants the research itself and an assessment form. The form consists of nine questions to estimate the study's reliability and the reviewer's familiarity with the field of research. Reviewers who consider themselves very familiar with the research area are expected to provide more reliable validation than those who consider themselves unfamiliar. However, since the reviewers themselves are all from areas related to cybersecurity, all responses are considered valuable. All questions are a combination of a number between one and five and a comment field.

The reviewers are all professors with their own tight time schedule, so it was decided not to submit the full paper in the first instance but instead a summary paper. Reading the full paper would take several hours of their time, affecting their willingness to participate. Therefore, a summary paper was created that would reduce the review time to approximately 30 minutes.

E.2.2 Bias Prevention

The nine questions of the assessment form and their formulation are all based on assessment forms of renowned academic journals in both general and cybersecurity fields, such as the *'Journal of Global Research in Computer Sciences'*. It is assumed that reputable scientific journals formulate their questions in a way that avoids bias. This ensures that the questions are objective without guiding the answers to specific answers.

E.2.3 Result Interpretation

The completed assessment forms are analysed by looking at the ratings given by the reviewers and their comments. The complete list of comments is found in appendix E. Only the notable comments are given in section 8.3. These noteworthy comments are comments that were either been repeated by multiple reviewers and/or are essential to improving the quality of the study.

This interpretation and analysis will be made separately for each question of the review. Hereafter, the most important aspects of this analysis are repeated in the conclusions and used to improve the study.

E.3 Results & Analysis

E.3.1 Results

Review requests have been sent to seven professors in various sub-disciplines of cyber security. As seen in Table E1, six of these professors accepted the request, and five returned the assessment form.

Table E1: Replies on review request

Reviewers	
Contacted	7
Accepted	6
Provided Review	5

E.3.2 Analysis

Each of the questions will first be given in the analysis, and then the results will be discussed. An exception is made for the first three questions as they are intended to assess the suitability of the review panel to validify the study.

Table E2: Question 1

Q1: "How would you rate your own expertise with Cyber Security?"		
Minimum	4	**Remarkable Comments:**
Average	4.75	
Maximum	5	

Table E3: Question 2

Q2: "How would you rate your own expertise with E-Commerce?"		
Minimum	2	**Remarkable Comments:**
Average	2.5	
Maximum	3	

Table E4: Question 3

Q3: "How would you rate your own expertise with governmental projects?"		
Minimum	2	**Remarkable Comments:**
Average	3	
Maximum	4	

From the first three questions, it is possible to assess whether the selection of reviewers has created a suitable panel for an expert review on the different aspects of this study. The first question already shows that the reviewers deem themselves perfectly capable of assessing cyber security. While some of the reviewers have noted that they are not well versed in some aspects, there does not seem to be a blind spot.

However, with regard to E-commerce and governmental projects, the reviewers are less confident in their assessment skills. Nevertheless, among them, enough reviewers deem themselves competent. Furthermore, this question came after the question of their cyber security expertise. Therefore, it is imaginable that the reviewers answered this question in light of question 1, and the rating might be given as a relative figure to their cyber security expertise.

Table E5: Question 4

Q4: "Are the study design and methods appropriate for the research?"		
Minimum	2	**Remarkable Comments:** ➢ Unclear how risk impact is being assessed ➢ Privacy aspect is underrated. Issues like price discrimination could arise. ➢ Unified killchain method could be inappropriate. This is because it is new and possibly non peer-reviewed.
Average	3	
Maximum	4	

Question 4 assesses whether the choice of methods was suitable for this study. It appears from the comments of some reviewers that this question has been mixed with the next question. The first noteworthy comment concerns how the risk impact is estimated. Currently, a risk is assigned an impact level based on its destructive effect, as described in chapter 7. However, due to the summary of the study, this detail was not properly explained in the paper. This will be further clarified as a result of the feedback in this study.

The following comment deals with privacy aspects. The privacy aspect is indeed underrated in this study. This study only looked at privacy as a means of identification, while it could also be used as an aid, for example, price discrimination. This shortcoming is mitigated by the system's structure itself, as it can be set up, so that transaction partners only need absolute required information. This would be their identification number. Only police investigators can obtain further privacy information on the basis of the identification number. However, this does not resolve the whole privacy problem as this system too can be misused, similar to cookies. More research needs to be done in this area, especially as there are many different perspectives possible.

The third comment points out that the unified killchain method is still new and may not be peer-reviewed. Both points seem to be true. The unified killchain method dates back to 2017, making it only four years old at the time of this study. However, this does not necessarily mean that it is not yet reliable in the fast ICT world. The more pressing issue is that the unified killchain method has not yet been peer-reviewed. A whitepaper was presented in early 2021, but it has not been peer-reviewed either. It is somewhat surprising that the unified killchain method has not yet been peer-reviewed because the underlying methods have been peer-reviewed.

Although the unified killchain method has not been peer-reviewed, it still shows its composition of multiple other killchain methods. This composition is reversible; it is also possible to derive another killchain variant based on the steps of the unified killchain method. In anticipation of a peer review of the unified killchain method, it is suggested that the assessment also uses another killchain method to assess whether this leads to significantly different results. Since the unified killchain method is closely related to these other killchain methods, no significant difference is expected.

Table E6: Question 5

Q5: "Are the methods used adequate and well used?"		
Minimum	3	**Remarkable Comments:** ➢ Choice for Killchain methodology unclear ➢ Decision for which attack patterns to use unclear ➢ Literature study provides generic sources ➢ Regulation 2015/1502 not well translatable into concrete requirements
Average	3	
Maximum	3	

For the fifth question, four comments were given. The first two points also relate to the vulnerability assessment. Both will need clarification, as the summary paper has not been clear enough on these. These comments are incorporated in chapter 5.

The next comment concerns the literature study. The literature study yields generic sources. This is something that was identified in this research as well. This field of research is fairly new, and therefore, not much can be found in a literature study in this field. With the exception of the aforementioned EU Regulations on this, the only sources available are of a general nature. Because this research is limited to the currently available sources, not much can be done about it. Since the Dutch government has not set up a committee until early 2021, and other nations have yet to start, it is expected that few specific sources exist at the moment. Therefore, it is difficult to take action on this point of comment.

This also partly applies to the following comment. Regulation 2015/1502 does not translate too well into concrete requirements indeed. However, this is not accidental but done by design. The EU attempts not to be restrictive in its regulations and gives the Member States margins to design their own system. If the EU regulations were too specific, this margin would not exist and obtaining consensus between the Member States would be almost impossible. For more specific information, national requirements will have to be consulted. However, these are not yet available at the moment. The main objective of this study is to indicate what amendments states should make to their national requirements to improve cyber resilience. This research is conducted on the assumption that specific information may not be available.

Table E7: Question 6

Q6: "Are the results clearly explained?"		
Minimum	2	**Remarkable Comments:** ➢ Unclear how drivers are distilled into crown jewels ➢ Privacy interests could be explained in context of businesses ➢ Vulnerabilities are hard to understand
Average	2.75	
Maximum	3	

Ambiguities in the method have already been discussed for the previous questions. This ambiguity naturally affects the results. Reason to pay attention to this aspect when modifying the relevant text sections. The only exception to this is the importance of privacy in the context of businesses. This privacy interest requires further investigation. This is, as explained earlier, indeed a shortcoming of this research and requires more future research.

Table E8: Question 7

Q7: “Are the results coherent?”		
Minimum	3	**Remarkable Comments:** ➢ Difficult to assess, results are on different abstraction levels ➢ Relation between different results unclear
Average	3	
Maximum	3	

Two comments were given for question 7. For the comment on different levels of abstraction, a reference is made to the risk assessment, also mentioned under Q8. This will be answered in detail under this question. For the second comment, it is sufficient to mention that the text is modified at this aspect.

Table E9: Question 8

Q8: “Are the results plausible if the methods used are taken into account?”		
Minimum	2	**Remarkable Comments:** ➢ Uncertain if list of vulnerabilities is complete ➢ Risk estimation methodology is unclear ➢ Aspects of private data when contracting company in DoS defence are not considered ➢ Impact of vulnerabilities could differ from estimations
Average	2.625	
Maximum	3	

The comments about the plausibility of results overlap a lot with the comments on the other questions. For example, the lack of clarity on whether the list of vulnerabilities is complete seems to correspond to the doubts on the choice of the unified killchain method. Therefore, this remark supports the earlier suggestion to investigate an alternative method for the unified killchain. However, this research will clarify its reasoning on why it believes the list is complete as well.

The risk estimation method was explained in significantly less detail in the summary paper. This probably contributed to its ambiguity. The method is already described in more detail in this report than in the summary paper, but it will be further elaborated to avoid any additional ambiguities.

When companies are contracted for DoS defence, privacy aspects are not considered. So, the comment made is valid. Additional research is not necessary for this comment. Chapter 7 specifically states that prior to a DoS attack, the government should have already concluded contracts with companies for the necessary emergency backup capacity. As part of these contracts, according to the basic principles of the GDPR, the government will have to add measures to ensure that privacy is guaranteed. Thus, the following phrase should be added: “The contract must contain measures to protect privacy”.

The impact of vulnerabilities could indeed differ from the estimations given. The comment made specifically mentioned the example of DoS impact and authority organisation attacks. In the summary paper, the details on the criteria for each level of impact were not explicitly mentioned. These details are given in this report. Based on the reviewer’s arguments, it was determined that the DoS would not meet these impact criteria as proposed by the reviewer. The other criteria would require a change in the impact classification, and accordingly, its risk. The impact of vulnerabilities is strongly influenced by the type of criteria used for labelling. It is likely that unless actual numbers can be calculated, their exact denomination can be subjective. These numbers cannot be accurately calculated until the system is actually implemented. Until then, some disagreement over impact levels is expected.

Table E10: Question 9

Q9: "Do you have additional remarks not covered by the other questions?"		
Minimum	-	**Remarkable Comments:** ➢ In the different abstraction levels, there's a gap which makes it harder to understand ➢ Decision for which attack patterns to use unclear, suggested use of MITRE ATT&CK framework ➢ Method and conclusion too much generalisation, therefore missing some steps
Average	-	
Maximum	-	

All additional comments have already been covered by the other questions. It is, therefore, unnecessary to discuss them again.

E.3.3. Amendments based on analysis

As already mentioned, the comments given by the review panel will be processed. This will be done in three ways:

1. Comments where something is considered unclear will be edited in the report to clarify it for future readers. These comments do not change the core of this study.
2. For the comments that require adjustments but no additional research, a list of changes will be presented. The changes themselves will not be integrated into the chapters of this study.
3. The comments that require additional research will not be addressed in this study. Instead, they will be given as recommendations for future research in this field.

Table E11: Research amendments

Category	Actions
Clarified in research	➢ Impact assessment method ➢ Choice for killchain method ➢ Risk estimation method ➢ Choice in attack patterns ➢ Relation between results ➢ Arguments that vulnerability list is complete
Amendments to research	➢ "The contract should contain measures to ensure the privacy protection of the private data." Added to the requirement related to emergency server capacity found in chapter 8 ➢ Impact rating of DDOS changed to medium. Risk level accordingly adjusted to high. No amendments to its suggested treatment.
Suggested future research	➢ Research into risks and interests of privacy aspects ➢ Validation with alternatives to Unified Killchain method such as MITRE ATT&CK ➢ Validation of actual national requirements after their publication