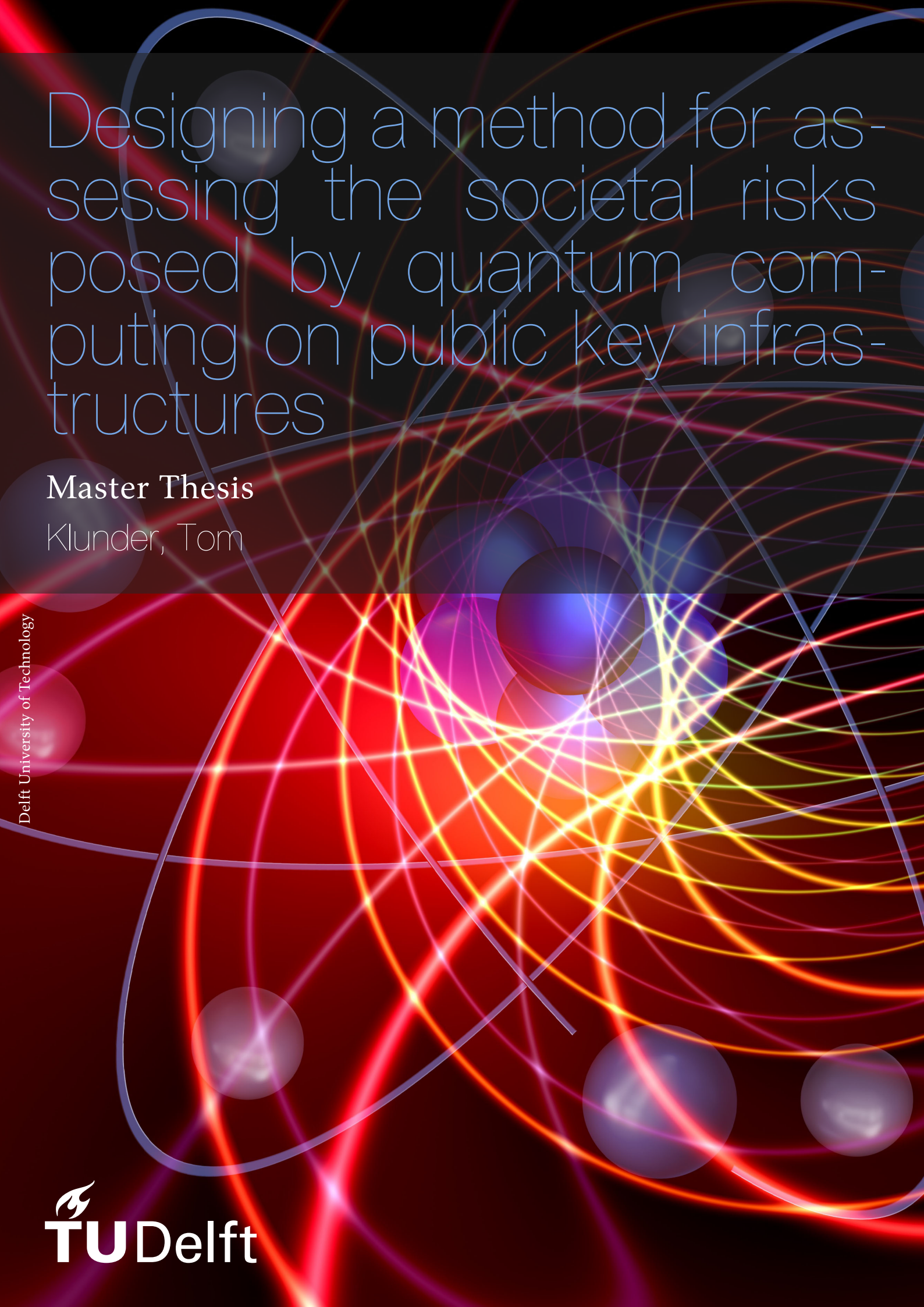

Designing a method for assessing the societal risks posed by quantum computing on public key infrastructures

Master Thesis

Klunder, Tom

Delft University of Technology

TU Delft

Designing a method for assessing the societal risks posed by quantum computing on public key infrastructures

by

Klunder, Tom

to obtain the degree of Master of Science
in Complex Systems Engineering and Management
at the Delft University of Technology,
Faculty of Technology, Policy and Management,
to be defended publicly on Tuesday June 21, 2022 at 14:00.

Student number:	4481607	
Project duration:	November 10, 2021 – June 21, 2022	
Thesis committee:	Prof. dr. ir. N. Bharosa,	TU Delft, supervisor
	Dr. P. E. Vermaas,	TU Delft
	Dr. M. H. A. Klaver,	TNO

Cover:	Quantum Physics. Original public domain image from Wikimedia Commons under CC0 1.0 (Cropped)
Style:	TU Delft Report Style, with modifications by Daan Zwaneveld

An electronic version of this thesis is available at http://repository.tudelft.nl/.

TU Delft

Preface

Dear reader,

I would like to take this moment to thank some people. First of all, I'd like to thank my graduation committee and the people in project HAPKIDO for giving me this amazing opportunity and working with me so passionately over the last few months. I'd like to thank the TU Delft and the staff of TPM for providing me with a greatly valuable education. I'd like to thank my parents and (little) brother for providing me with a solid base to fall back to, without being overbearing. I'd like to thank my housemates, friends, and family for providing a stimulating environment in which I could unwind as well as be encouraged to keep on going.

Again, thank you all for your unwavering support and patience through this at-times trying process. I could not have done this without you. Even though it may not always seem like it, I really do appreciate your practical help and the smallest gestures immensely.

Klunder, Tom
Delft, June 2022

Summary

Our digital society is heavily dependent on cryptography. Cryptography is the way information and communication are secured. It prevents eavesdroppers from listening in and ensures that received data is trustworthy, enabling trusted online transactions such as e-commerce and digital document signing. It means companies can do legally binding business with other companies online, a civilian can communicate sensitive information to their government via their web browser, and you can pay a Tikkie to your friend. In other words, modern cryptography is the basis for our digital society.

Online trust is for a large part made possible by Public Key Infrastructure: "a combination of software, hardware, roles, guidelines and procedures that are required to manage keys as digital certificates". In essence, Public Key Infrastructure is the application of cryptographic technology through institutions in the form of standards and the cooperation of actors. The application of Public Key Infrastructure for creating digital trust is widespread and interwoven in our society. It is extensively used in organisational identity management, internet (website & server) security, secure email, virtual private networks & intranets, software updates, the Internet of Things, healthcare, finance, and critical infrastructures.

At the core of Public Key Infrastructure is asymmetric cryptography. In turn, at the foundation of conventional asymmetric cryptography lie two mathematical problems. The hardness of these problems guarantees the security of the cryptographic schemes that use them. Reasoning back, the hardness of the two mentioned mathematical problems is what most digital trust systems, by using Public Key Infrastructure, depend on.

But what if these mathematical problems are not so hard anymore? If that is the case, the cryptographic schemes cannot guarantee information security. And if information security cannot be guaranteed anymore, there is no trust. Our society and economy depend on reliable digital financial transactions and confidential communications, which cease to exist without trust. Simply put, disaster would strike.

Such a scenario is made realistic by the dawn of quantum computing. Because of the fundamental differences in the way of computing when compared to classical computing, quantum computing is able to apply Shor's algorithm and make the two classically hard mathematical problems not hard. As quantum computing is still being developed, a large enough quantum computer to crack today's cryptographic standards does not yet exist. However, experts estimate the chance that it is developed before 2030 small but realistic. The Dutch General Intelligence and Security Service (AIVD) follows this vision. The quantum threat, meaning the looming ability to crack today's cryptographic standards and thereby break digital trust using quantum computing, is real.

It is clear that the quantum threat materialising will have shattering effects to society. However, it is not described in literature what exactly society will feel, aside from relatively general statements about areas impacted. Rather, most studies focus on the technical impacts. There is a need to know more about the potential societal effects, so (1) it becomes clear how pressing the matter of the quantum threat is and (2) where to focus energy to avoid the worst effects.

Research objective

With these two aims of knowing the potential societal effects of the quantum threat to Public Key Infrastructure in mind, this research seeks to establish a method to assess these effects. In other words, the objective of this research is to develop and test a method for assessing the societal risks of quantum computing, in particular focusing on domains that use Public Key Infrastructure systems.

In doing so, this thesis contributes to the research project HAPKIDO. HAPKIDO aims to investigate the transition towards quantum safe public key infrastructure by treating the transition as a governance as well as a technical problem. This thesis is part of work package 1 of project HAPKIDO, aiming to investigate the societal risks of quantum unsafe public key infrastructure when quantum computing is largely available.

Due to practical constraints, this research is limited to qualified trust services as defined by the eIDAS regulation within the Netherlands. The reason for this scope limitation is that eIDAS regulation very clearly delineates what a trust service is and where the liabilities lie.

An important distinction to make in potential societal effects are those that result from Public Key Infrastructure failing because of the quantum threat and those that result from mitigation and migration efforts. This research is limited to the former. As such, potential solutions to the quantum threat such as quantum key distribution, post-quantum cryptography, and hybrid cryptography are out of scope.

With the objective and the scope of the research set, the following research question is defined: *What are the components of a method to assess the potential societal effects of the quantum threat to Public Key Infrastructure used by qualified trust service providers? (RQ1)*. An additional research question that helps validate the answer to the first research question and is interesting as an exploratory venture is: *What are the potential societal effects of the quantum threat to PKIoverheid in the Netherlands? (RQ2)*.

Research approach

To answer the first research question, this research is based on Design Science. The three Design Science research cycles are present by continuously drawing from literature, iterating versions of the artefact, and having multiple field test moments throughout the design process.

After several workshops with actors filling differing roles in the Dutch Public Key Infrastructure landscape concerning qualified trust services, the Societal Risk Assessment is complete. Applying the method explores the following:

- Risks to the assessing organisation
- Risks to society that are within the sphere of influence of the assessing organisation
- Risks that arise from the presence of the quantum threat
- Risks related to information security compromise in Public Key Infrastructure structures
- Impacts of not being able to guarantee information security in Public Key Infrastructure structures, rather than definite compromise

Findings

The Societal Risk Assessment consists of six steps: determining the scope, identifying the threats & vulnerabilities, identifying the assets, assessing the impacts, assessing the likelihood, and lastly the synthesis. Each step produces knowledge necessary to arrive at the outcome: an overview of risks to the organisation and to society within the sphere of influence of the assessing organisation. This

answers the first research question. This Societal Risk Assessment is, to the best of my knowledge, the first of its kind, combining risk assessment in information security with the consequences to society. This is important in a world ever increasingly dependent on digital communication.

The following statements summarise the application context of the SRA:

- The SRA can be applied by any party that is reliant on PKI and wants to know the risks they run in a societal context because of their PKI reliance.
- The SRA is designed to be domain unspecific and is expected to work similarly across domains.
- It is advised to perform the assessment with a team of experts with expertise in risk management, (senior) management, technology (i.e., PKI), potentially affected business processes, and compliance.
- It is advised that the assessment is guided by an assessment leader that is acquainted with the SRA method.
- The assessment is expected to take four to six hours.
- A report should be drawn up from the results of the assessment to maximise actionable insights.

It should be noted that although the SRA is expected to work similarly across domains, this has not been field tested. Further points on this are made in the reflections and recommendations. This also applies to the expected duration of the assessment and the best way to guide the assessment.

Workshops with intended future users of the Societal Risk Assessment, expert consultation, and a case study output evaluation session with experts concluded in two main beliefs about the Societal Risk Assessment: Firstly, the value of the Societal Risk Assessment as an assessment and its output is recognised. The second belief is that it can be difficult to apply the Societal Risk Assessment, as it requires time and varying expertise. Help during the application of the Societal Risk Assessment is absolutely necessary, to guide the expertise of non-risk management experts.

The case study that was done was from the perspective of Logius, as the policy authority of PKIoverheid. This answered the second research question: What are the potential societal effects of the quantum threat to PKIoverheid in the Netherlands? In short, there are a myriad of ways in which society may be impacted if Logius is not able to secure PKIoverheid. Examples include interference with information exchange for medical professionals; leaking of company secrets of many companies operating in the Netherlands; potential loss of any application that uses DigiD facilitating communication between the Dutch government and citizens; large scale fraud because accountants, bailiffs, and notaries cannot securely sign documents; and leaking of military intelligence, as secure communications are very hard to set up.

The first set of recommendations of this research is for organisations active in providing, maintaining, or making use of Public Key Infrastructure-enabled trust services. These organisations would do well to implement this Societal Risk Assessment or another way to include the quantum threat and their societal influence in their business continuity planning. Furthermore, I recommend them to look into the results of the following HAPKIDO work packages or the application of the Crypto Agility Risk Assessment Framework.

Secondly, I recommend researchers to improve the guidance offered and the impact estimation parts of the SRA. As for the rest of work package 1 in project HAPKIDO, I suggest an evaluation session with more and more diverse participants, before applying the Societal Risk Assessment in other domains and potentially again in the eGovernment domain for rigour purposes.

Contents

Nomenclature

Abbreviation	Definition
BIA	Business Impact Analysis
CA	Certificate Authority
CARAF	Crypto Agility Risk Assessment Framework
CIA	Confidentiality, Integrity, and Availability
GRNV	Integrated Risk Analysis National Security
PA	Policy Authority
PKIo	PKI overheid
QC	Quantum Computing
QS	Quantum Safe
QTSP	Qualified Trust Service Provider
RA	Risk Assessment
SecRAM	Security Risk Assessment Methodology
SIA	Social Impact Assessment
SRA	Societal Risk Assessment
SWOT	Strengths, Weaknesses, Opportunities, and Threats
TSP	Trust Service Provider

1

Introduction

Quantum computing is an exciting new technology with much potential for tackling computational problems that conventional computing cannot. If harnessed, it promises to provide great computational power facilitating scientific breakthroughs in many fields (Gill et al., 2021; Vermaas, 2017). However, while it is expected to provide benefits in the field of cybersecurity, it is simultaneously expected to threaten the security of our digital society (Raban & Hauptman, 2018). This may seem paradoxical, but it is not.

Currently, most online communication is secured by leveraging cryptography that is infeasibly hard to break. The industry standard cryptographic schemes can theoretically be broken, but this takes thousands of years in practise. After decades of trying, nobody has found a way to do so in a reasonable time. Therefore, the current standards are *reasonably* secure, but not *provably* secure. After all, there is a chance that somebody comes along who does find a way to break the cryptographic schemes quickly. It seems that time is soon to come. Whilst it is not capable yet, quantum computing is fully expected to break the current standard cryptography quickly. The cryptography that we rely on so much to secure our online communications. This greatly threatens the security of our digital society. On the other hand, quantum computing is expected to provide ways in which online communications can be provably secure. Provable security is a big improvement over reasonable security, as it excludes all possibilities of the security being broken. With provable security, a scenario such as quantum computing breaking online communication security cannot come to be. This is how quantum computing both threatens and promises to improve cybersecurity. The rest of this thesis will focus on the threatening part of the equation.

It is established that quantum computing will threaten cybersecurity by breaking modern cryptographic standards. This is called 'the quantum threat'. However, why is this an issue? Part of the cryptographic standards is public key infrastructure (PKI). PKI is "a combination of software, hardware, roles, guidelines and procedures that are required to manage keys as digital certificates" (Bharosa et al., 2015, p. 263). Essentially, it is a way to put cryptography as a technology to use and create digital trust. This is where the transition from pure technology to societal merit happens. Current cryptographic standards, PKI, and the technological consequences of quantum computing on cryptography are further detailed in . For now, we focus on the role of cryptography in society. PKI plays a crucial role in digital society as we know it. It allows online authentication so that only you can access your social

media account[1], secure communication of sensitive data such as between medical professionals, and legally binding electronic signatures or financial transactions. PKI usage is very much interwoven in many if not most of our online activities, especially those that require trust. One can imagine that this societal dependency on a vulnerable technology can have potentially disastrous consequences.

1.1. Unknown societal risks

The technological consequences are explained above, but in what ways this will impact society is less clear. Moreover, rather than societal consequences, this research investigates the societal risks of quantum-unsafe PKI. The term risk is more suitable, as it implies on the one hand an element that we would like to protect and on the other hand uncertainty. This applies as digital trust and its benefits are the things of value that we would like to protect and there is great uncertainty surrounding the development of the threat: a large enough quantum computer to break current public key cryptography standards. The societal risks are not clearly known, which increases the vagueness of the problem at hand. A vague problem causes issues in solving it. There is a need to know more about the societal risks, so (1) it becomes clear how pressing the matter of the quantum threat is and (2) where to focus energy to avoid the worst effects. By (1) creating a shared picture of what the societal risks are in cooperation with actors involved with PKI, the problem perceptions of these actors start to align. The alignment of problem perceptions bolsters actor commitment to solving the matter at hand in cooperation (Bruijn & Heuvelhof, 2008). This is particularly necessary in the case of the quantum threat to PKI, as PKI inherently involves many actors with differing roles in the trust chain. The other benefit of knowing the societal risks is that (2) it helps preparing for the transition to a solution. Logically, by knowing what specific instance of PKI causes the worst societal risks, you know where to prioritise in mitigating the quantum threat. Focusing on a prioritisation strategy is recommended in transitioning to a quantum safe systems (Joseph et al., 2022). These two points clearly show the societal relevance of knowing the societal risks of the quantum threat.

1.2. Societal Risk Assessment

The problem is that there is little research on the societal risks of the quantum threat to PKI. This is shown by the literature review in Section 3.5. Therefore, this research is all the more necessary. Additionally, there is no developed method available to assess the societal risk. This research aims to provide a method to assess these risks: a Societal Risk Assessment (SRA). In other words, the objective of this research is to develop and test a method for assessing the societal risks of quantum computing, particularly in domains that use PKI systems.

In the previous section, the societal relevance of knowing the societal risks of the quantum threat is established. Consequentially, providing a sound method to uncover the societal risks is of societal relevance as well.

1.3. Scope

As this research is a part of project HAPKIDO, it takes on some scoping choices from the project for practical reasons. The project's goal is to research how to transition to quantum safe PKI in the Netherlands. Therefore, this research will also focus on the Netherlands. Secondly, this research will focus on PKI as opposed to public key cryptography in general. More specifically, this research limits itself to PKIs with a hierarchical trust model. PKI is the applied form of public key cryptography, generating trust necessary for societal applications. Secondly, the hierarchical trust model is a very widely

[1] Dismissing the possibility that somebody else knows/guesses your login credentials

adopted paradigm (Amadori et al., 2022). These two arguments justify the scope choice as the societal risks of the quantum threat will be most significant when considering PKIs with a hierarchical trust model.

Another scoping choice is to consider only qualified trust services as defined by the European eIDAS regulation. eIDAS regulation is being adopted throughout the EU standardising trust services. Market parties expect the need for higher levels of trust, and thus qualified trust services, to keep growing. As the quantum threat is a threat of the future and qualified trust services are expected to become the solidified standard, the scoping choice makes sense. Additionally, qualified trust services have the strictest requirements, providing the most trust, and therefore are likely to have the largest societal impacts if that trust is broken. These are provided by Qualified Trust Service Providers (QTSPs). This scope excludes self-signed CAs used for applications within an organisation. It is assumed that these internal applications are more easily adapted to deal with the quantum threat, as there will be less governance struggles because there is no large actor network involved. Therefore, they are less relevant to finding the most important societal risks. The same holds true for symmetric cryptography as opposed to asymmetric cryptography. Symmetric cryptography is less vulnerable to the quantum threat and applications using it can be relatively easily adapted when compared to asymmetric cryptography. Thus, the scope of this research is set to asymmetric cryptography.

1.4. Research questions & scientific relevance

With the objective and the scope of the research set, the following research question is defined: *What are the components of a method to assess the potential societal effects of the quantum threat to PKI used by QTSPs?* (RQ1). An additional research question that helps validate the answer to the first research question and is interesting as an exploratory venture is: *What are the potential societal effects of the quantum threat to PKI Government in the Netherlands?* (RQ2).

Whilst the societal relevance of this research is apparent, the answers to these two questions also provide scientific contributions. As mentioned in Section 1.3, this thesis is part of a larger research project: HAPKIDO. HAPKIDO aims to investigate how the transition towards quantum-safe PKI can be realised (Spini, 2020). It recognises that this is not just a technical, but also a governance challenge. It hopes to achieve its goals by involving a consortium of actors with a wide variety of expertise. This includes actors with "fundamental knowledge on cryptography; transitional governance; system design, integration, and implementation; experience with PKI requirements; and knowledge on how the PKI systems are used by PKI-users" (Spini, 2020, p. 10). HAPKIDO is divided in nine interlinked work packages. These and their relations are displayed in Figure 1.1. This research is part of work package 1: Societal Impact Assessment. While the later work packages are concerned with questions on what to do, the main research question of this work package is *What are the societal risks of a quantum unsafe PKI in the quantum era?* The answer to this question lays the basis for stakeholder engagement throughout the project. The two research questions of my thesis clearly build towards an answer to the main research question of work package 1. The answer to RQ1 helps to set up a method that can be used to answer the work package 1 question and the answer to RQ2 is a partial answer, as it answers the work package 1 question for solely PKI Government.

Aside from project HAPKIDO, this SRA is—to the best of my knowledge—the first risk assessment to bring information security risk of technological infrastructures and the impact to society together. As presented in the literature review, there have been plenty of information security risk assessments and there have also been methods to gauge societal impact, but they have not been combined before. This is ever relevant in a world increasingly reliant on digital means and online transactions, especially in

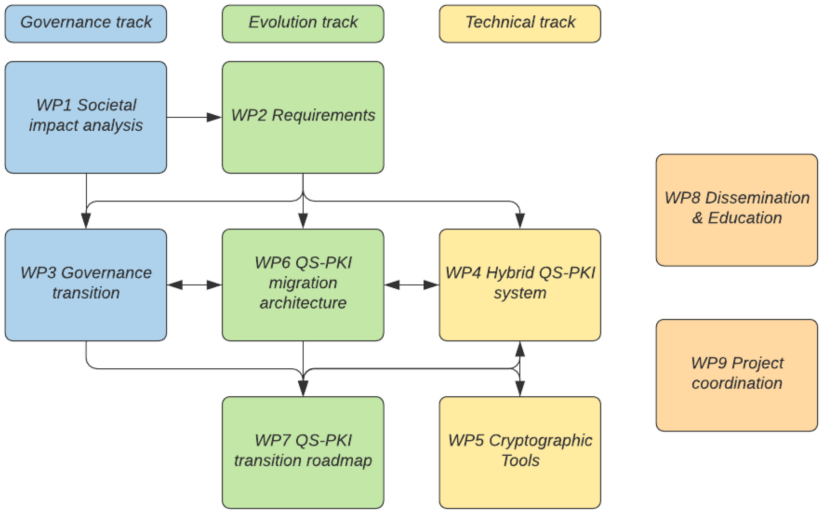

Figure 1.1: HAPKIDO work packages (Spini, 2020)

face of the quantum threat.

When relating the scientific contributions of this thesis to theory, both design science research and risk analysis are relevant. In design science research as defined by Hevner et al. (2004), the conceptual knowledge base consists of all explicit and tacit knowledge relevant to the designer. This is further explained in Section 2.1. By answering RQ1 and RQ2, this research adds to this knowledge base and provides knowledge that can be used in future (design science) research or practically in the application domain. In terms of risk analysis science as defined by Aven (2018), the scientific contribution of RQ1 is of type B knowledge and that of RQ2 is of type A knowledge. What this means is detailed in Section 3.7.

In the rest of this thesis, first the methodology is laid out in Chapter 2. After that, the literature review is presented in Chapter 3 and then the SRA in Chapter 4. Next in Chapter 5, a case study and evaluation of the output of the SRA is discussed. Lastly, the conclusions, reflections, and recommendations are laid out in Chapter 6.

2

Methodology

2.1. Design Science as a research approach

In this research, there is a need to design. RQ1 calls for an approach that can help to create an SRA and make it so that an effective SRA is the outcome. The Design Science research approach as described by Hevner et al. (2004) and elaborated upon later by Hevner in 2007 is a good fit. There are three cycles that should be apparent in good design science research. These are the relevance cycle, the rigour cycle, and the design cycle. These are depicted in Figure 2.1.

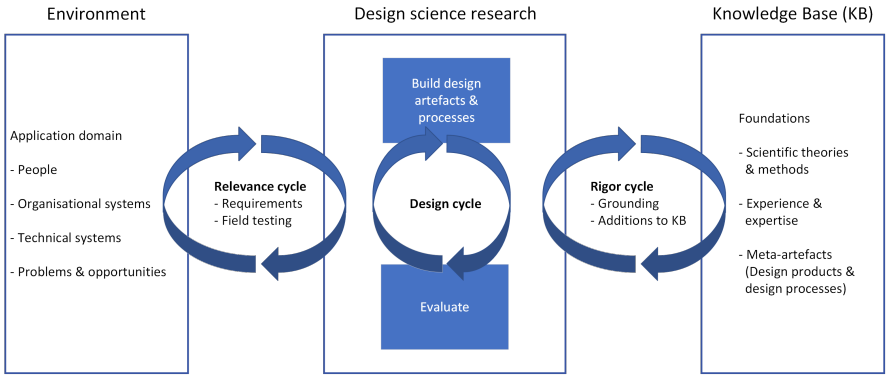

Figure 2.1: Cycles in design science research (Hevner, 2007)

The relevance cycle connects the designing activities with the application environment of the research project, so that relevancy of the research is ensured. Usually, design science research spawns from problems or opportunities in an application environment. When the need for an artefact arises, it initiates the design process. An artefact is the artificial 'thing' to be designed. In the case of this research, there is a need for an SRA that emerges from the context of our digital society vulnerable to the quantum threat. Therefore, the SRA is the artefact. After the initialisation, the relevancy cycle serves to keep the artefact being designed connected to the contextual reality. This happens throughout the design process, so that the artefact will be well adjusted to the contextual needs and thus useful.

The rigour cycle draws existing knowledge from the knowledge base to fuel the design process. This knowledge base consists of expertise, pre-existing artefacts, and theories. Then the lessons learnt and

artefacts produced during the design process add to the knowledge base. The design science researcher should explore the state-of-the-art in the application domain, so that the design science research may provide scientific knowledge contributions rather than routine design. In this research, it is absolutely necessary to learn from previous risk assessment methods and theory to come to an effective SRA.

The last of the three cycles is the design cycle. This cycle is at the core of the design science research. It iterates between generating new design alternatives and evaluating them and considering which way to proceed with the artefact. To support these activities, the design cycle takes input from both the relevance and the rigour cycles as described above. In turn, it provides input to the other two cycles as well. The intermediary artefact is used in the relevance cycle for field testing and its results steer the design cycle. The artefact is based on lessons from the knowledge base and adds lessons obtained during the design process to the knowledge base in the form of experiences from field testing, extensions of theories, and new artefacts. An adaptation of Hevner's design science research cycles specific to this research can be found in Figure 2.2. The adaptations made are explained in the rest of this chapter.

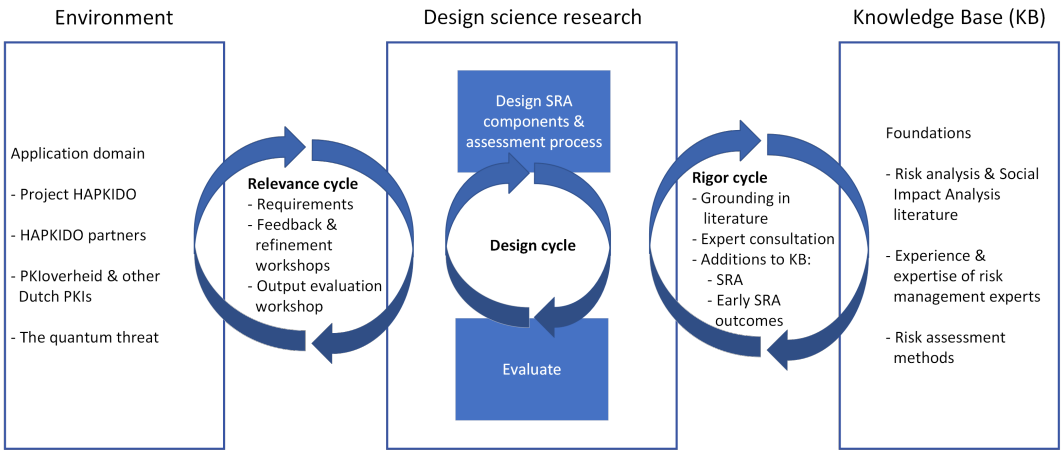

Figure 2.2: Design science research cycles in this thesis, adapted from (Hevner, 2007)

2.2. Literature review

In this research, the rigour cycle from Hevner's model (2007) partially takes form as a literature review. The literature review was a continuous process looking into several knowledge domains. These include quantum computing, the quantum threat, current cryptographic standards, social impact assessment, and risk analysis. The Scopus and Google Scholar databases were used to search for relevant literature. The snowballing method is applied to find newer and older publications.

The first part of the literature review is part of the relevance cycle. As described in Section 2.1, the design science research is initiated by the need for an artefact that stems from a problem in the application context. In this case, the problem is the lack of insight into the societal risks posed by the quantum threat. To better understand the application context and thus increase the relevancy of the SRA, the current cryptographic standards and how they are threatened by quantum computing are explored. Additionally, an attempt is made to explore literature on the societal effects of the quantum threat, or rather the lack thereof.

Then, the literature review investigates ways in which the (societal) effects of technology are assessed. To do so, literature on risk analysis and on societal impact assessment is consulted. From this literature, lessons are drawn to support the structure and building blocks of the SRA. This is an apparent

expression of the rigour cycle. The results of the literature review are presented in Chapter 3.

After a first exploration of the potential methods that may serve as inspiration to the SRA, a draft version of the SRA was made. This very first version served as a stepping stone to later iterations based on feedback from intended users and field experts. This feedback was gathered in workshops.

2.3. User workshops

The larger part of the relevance cycle is embodied by a set of workshops with the intended user-base of the SRA. These workshops were set up to gather input from the participants and align the SRA with user needs. In total, five of these workshops were held. Participants were selected based on their activity in providing, maintaining, or making use of PKI-enabled trust services, their accessibility through the HAPKIDO project, and the fact that they work in varying sectors (i.e., eGovernment, banking, and telecom/commercial trust service provision). Table 2.1 provides an overview of the user workshops that were held. A schematic overview of how the workshops are related is presented in Figure 2.3. The SRA output evaluation workshop in this figure and its purpose is described in Section 2.5.

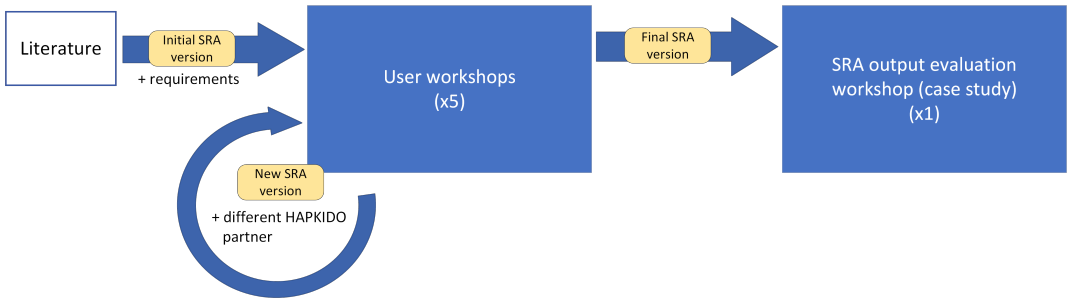

Figure 2.3: Schematic overview of workshops

Every user workshop took around 90 minutes and started with a brief introduction of this research and then some interview questions on the use of PKI within the organisation of the participant(s). Then, the main part of the workshop consisted of going through the SRA step-by-step, seeing how the participants react and asking for feedback on how each step can be improved. Lastly, there was room for a short discussion on what the participants thought of the SRA and its usefulness.

Every workshop serves as an opportunity for evaluation of the design requirements and the artefact in the process of being designed. After every workshop the SRA is refined and the refined artefact is used as input for the next workshop. To structure the feedback from every workshop, the researcher used the SWOT analysis technique. Using this technique allows for bolstering the strong aspects of the artefact and improving the weak aspects. The SWOT table for every workshop and the subsequent choices regarding the SRA can be found in Appendix B. This constant evaluation and iteration of adjustments after every workshop resembles the design cycle.

2.4. Expert consultation

To further bolster the research, expert consultation was done throughout the research process. In the design science research framework, expertise and experience are part of the knowledge base (Hevner et al., 2004). Four experts were selected based on their knowledge on information security risk, familiarity with PKI, and accessibility through the HAPKIDO project. The four experts were a governmental technology professor at Delft University of Technology, an information and critical infrastructure security scientist at TNO, a strategic advisor information security and risk management expert at TNO,

Table 2.1: Overview of workshops

User Workshop	SRA version	PKI domain	Participants	Date
1	0.1	Government	PKI manager at PA, manager at TSP, PKI researcher	02-11-2021
2	0.2	Banking	M2M communication program lead at a large bank	13-12-2021
3	0.3	Telecom	PKI manager at QTSP, compliance officer at QTSP, technical expert at QTSP	12-01-2022
4	0.4	Government	M2M communication program lead at tax authority, risk management expert	26-01-2022
5	0.5	Government	PKI manager at PA, cyber security scientist	24-02-2022
Evaluation workshop	1.0	Government	PKI manager at PA, two cyber security scientists, government and technology researcher	13-04-2022

and a cybersecurity scientist at TNO. Expert consultation was done to elicit their tacit knowledge for use during the design process. This is part of the rigour cycle.

The consultation occurred in two forms: semi-structured interviews and participation in the user workshops. In total, six semi-structured interviews were held with experts present in varying composition. The goal of these interviews was similar to that of the user workshops: to improve and validate the SRA. Part of the user workshops was attended by some of the experts. The composition of participants for each workshop can be found in Appendix B.

2.5. Case study: Logius and PKIoverheid

After a few design cycles, the SRA is ready to be field tested. This is done by using an instrumental case study. Doing so achieves two goals. Firstly, it provides an evaluation of the outcome of the design process. Evaluation of the artefact is necessary in good design science research and doing a case study is one of the ways to achieve that (Hevner et al., 2004). This helps to solidify the answer to RQ1. Secondly, the case study has the goal of providing insight into the societal risks that the quantum threat poses to PKI. The instrumental case study is not specifically done to investigate the outcome of the specific case, but to provide insights that may be applicable to other cases as well (Stake, 2003). In this research, applying the SRA to a typical case that the SRA is intended to be used for is helpful to see how well this can be done, which is also relevant for other cases. Similarly, applying the SRA to a single assessing organisation may reveal understanding of societal risks that other organisations run as well. By having Logius and its role in PKIoverheid as the case, the case study provides an answer to RQ2.

This research investigates the case of Logius and its role in PKIoverheid. The reason for this is that Logius is easily accessible through the HAPKIDO research consortium and is expected to be used to think about their societal impact, as they are a governmental agency. PKIoverheid is the PKI of the Dutch government facilitating secure communication between the public sector, private sector, and citizens. This means that the quantum threat is likely to cause a broad range of societal risks in the case of PKIoverheid. Logius, being the policy authority of PKIoverheid, is in charge of safeguarding the trustworthiness of the entire infrastructure. Therefore, it is a prime candidate for analysis. The case is further described in Section 5.1.

Table 2.2: Case study output evaluation statements

Statement	Related evaluation criterion
The SRA gives a complete picture of the relevant risks	Completeness
The SRA provides the right level of granularity	Quality of results obtained
The SRA is simple to understand	Simplicity
The SRA is easy to use	Ease of use
People need help using this SRA	Ease of use
The SRA produces actionable insights	Quality of results obtained
I would recommend this SRA to colleagues	-

Unfortunately, due to time constraints, the SRA could not be applied in a workshop by the participants themselves. The SRA was applied by myself to the case of Logius as the Policy Authority of PKIoverheid. Then, the filled in SRA was given to four participants in advance to a workshop. The participants consisted of one manager at Logius, one researcher in the field of government and technology, and two cybersecurity researchers familiar with risk assessment. In this workshop, contrary to the previous workshops, the goal was to evaluate the produced output of the SRA, rather than the steps of the SRA itself. The larger part of the workshop consisted of going through the output for every step of the SRA. Then, the participants were asked to score on a 7-point Likert scale how much they agreed with a few statements about the SRA and its output. These statements are based on the evaluation criteria for methods proposed by Gregor (2006): completeness, simplicity, consistency, ease of use, and quality of results obtained from use of the designed method. The statements can be found in Table 2.2. Here, you can see that the consistency criterion is left out. This is because a risk assessment is inherently subjective and the output is heavily dependent on the assessor(s). It is my opinion that consistency should not be striven for, as the SRA needs to provide the freedom to the assessors to produce the output they feel is relevant at the time. Something else of note is the addition of the last statement: "I would recommend this SRA to colleagues". This statement does not reflect a specific criterion, but is a reflection of all criteria and the perceived fitness of the SRA as a whole to the participant.

During the last part of the output evaluation workshop, the participants were asked to collectively perform a SWOT analysis. The results of the case study and evaluation of the output are presented in Chapter 5.

3

Literature review

This literature reviews describes relevant literature found and how it relates to this research. First, the current cryptographic landscape and how it is threatened by quantum computing is described. Then, the limited research on the societal impact of the quantum threat is highlighted. After, the risk-related literature on which the SRA is based is analysed. All lessons drawn from the literature that are directly implemented in the SRA are summarised in Table 3.2.

3.1. Current cryptographic standards

The security of our digital society is largely dependent on cryptography. It is used to encrypt our data, from highly confidential state secrets to stored grocery lists for privacy reasons. By encrypting it with a shared secret, or a key, the data is rendered unreadable. Later, using the same key, the process can be reversed or decrypted, so that the original readable data is recovered. The original and age-old goal of cryptography is to ensure none other than the intended recipient can read the message. This is called confidentiality. There is only one currently known cryptographic cipher that is perfectly secure, meaning that it is theoretically impossible to break it. This is the Vernam cipher. This sounds like the perfect way to secure information, but there are two drawbacks.

The first drawback is key size. Using the Vernam cipher requires a key that is the same size as the data. This means that sending a confidential file of 200MB requires sending the file plus a 200MB sized key, effectively doubling the necessary capacity of electronic communication. This is extremely inefficient and thus not practical for day-to-day use. To solve this issue, many new ciphers were invented, leveraging computational problems. These are mathematical problems that cannot realistically be solved by conventional computers. Using all computational power in the world, breaking such ciphers would still take thousands of years. This means that even though the ciphers are not theoretically secure, they are practically secure.

The second drawback of the Vernam cipher is that it is a form of symmetric cryptography. The result is that in case of communication, it requires both parties (Alice and Bob) to know the key. This means that they need a way to securely communicate before being able to securely communicate. This is called the key distribution problem. One solution to this problem is asymmetric cryptography.

Asymmetric cryptography is a form of cryptography that uses key pairs, consisting of a private and a

public key. Alice can encrypt a message with Bob's public key, which can now only be decrypted with Bob's private key. This is also called public key cryptography. Public key cryptography is a necessity for secure internet standards such as TLS and PGP. The most popular form of public key cryptography is RSA, which relies on the hardness of prime factorisation. Other popular public key cryptography schemes are Diffie-Hellman and Elliptic Curve Cryptography. These rely on the hardness of the discrete logarithm problem. In case of both problems, computation becomes infeasible once the parameters (i.e., key size) are large enough.

Aside encryption, public key cryptography can be used for signing. Doing so proves that a certain message is written by the owner of the private key that belongs to a certain public key. Alice uses her private key to create a signature based on a message. Bob can then use Alice's public key and the signature to verify that it is Alice who signed the message. More information on cryptography and its workings can be found in the book Cryptography Made Simple by Smart (2016).

Observant readers may have noticed that public key cryptography requires knowledge beforehand as well. After all, how can you be sure that an insecurely communicated public key is in fact the public key of the intended recipient? There may not be a need for a shared secret, but there is a need for trust in the public key. This is where Public Key Infrastructure comes into play.

3.2. Public Key Infrastructure

There is a need for trust in that a certain public key belongs to a certain party. In the current digital landscape, this trust is provided by Public Key Infrastructure (PKI). PKI is "a combination of software, hardware, roles, guidelines and procedures that are required to manage keys as digital certificates" (Bharosa et al., 2015, p. 263). PKI is a system that brings together actors, using institutions and cryptographic technology to achieve digital trust. At the basis of PKI lies assumed trust in a trusted third party. This trusted third party signs the certificate (i.e., the public key) of Bob. Alice can now verify that the certificate presented by Bob is signed by the trusted third party. As Alice trusts the trusted third party, she can trust that the certificate presented by Bob is in fact Bob's. In this scenario, the trusted third party fulfils the role of root Certificate Authority (CA). There may be another party that is trusted by the root CA to sign certificates, which signs Bob's certificate. In this scenario the other party is an intermediary CA. The concept presented in this scenario is the chain of trust. It is crucial that CAs are strict in their policies that dictate which certificates are signed for whom, as otherwise trust is lost.

There are many parties active as root CA. Their certificates often come pre-installed on consumer devices and in web browsers. The collection of pre-installed certificates on a device or in an application is called the root store.

There are several functions that need to be fulfilled in a PKI by several roles. These include certificate usage, certificate revocation, certificate generation, and setting the rules for all of these.

Aside from confidentiality, there are other purposes that are enabled by PKI. These are the integrity of data, authentication of persons, organisations, and systems, and non-repudiation. Altogether they serve to enable trustworthy and legally binding electronic transactions. This in turn enables business and public administration to be conducted online, heavily improving the efficiency of society. This is evident from the massive adoption of PKI and its interwovenness in society. It is extensively used in organisational identity management, internet (website & server) security, secure email, virtual private networks & intranets, software updates, the Internet of Things, healthcare, finance, and critical infrastructures (Mulholland et al., 2017).

3.3. The quantum threat

Now that the current cryptographic landscape is clear, the vulnerability to quantum computing can be explored. As mentioned, the present-day digital trust relies on public key cryptography, which relies on the hardness of the prime factorisation and discrete logarithm problems. These two mathematical problems are hard for conventional computing. However, quantum computing presents a fundamentally different way of computing, which allows Shor's algorithm to be applied. This algorithm can efficiently solve both the prime factorisation and discrete logarithm problems. In turn, current public key cryptography provides no security, as it is easily broken in theory. For now, there is no quantum computer available with enough processing power to attack current public key cryptography standards. However, technological strides have been made over the past years which make the advent of such a quantum computer in the future very likely (Skosana & Tame, 2021).

When exactly the efforts of the scientific community will come to fruition is anybody's guess. There are many different views among experts of how long such endeavours will take. However, experts generally agree that it will happen eventually. In a report on the expected timeline of quantum computing, Mosca and Piani (2021) found that more than half of the inquired experts ($n = 44$) thought that such a quantum computer is unlikely to exist before 2030. On the other hand, a quarter thought that it was 50% likely or more. The near consensus found in the report is that the threat is likely to occur before 2040. 36/44 respondents indicated they ought the threat likely, very likely, or extremely likely to occur before 2050. The Dutch General Intelligence and Security Service (AIVD) follows this vision and advises parties that have an information security need to act accordingly (Algemene Inlichtingen- en Veiligheidsdienst, 2021).

All in all, there is a small but realistic chance that by 2030, and otherwise by 2040 or 2050, the foundation of digital trust will be no more. As illustrated before, our society and economy depend on reliable digital financial transactions and confidential communications, which cease to exist without trust. Simply put, disaster would strike (de Wolf, 2017).

3.4. Post-Quantum Cryptography & Project HAPKIDO

The vulnerability of conventional digital infrastructure to the quantum threat is a worldwide problem. In the United States, NIST is developing standards expected to be final by 2024 for new public key cryptography schemes resistant to quantum computing. To transition to quantum safe PKI in the Netherlands, the research project HAPKIDO is running. Solutions like Post-Quantum Cryptography, Quantum Key Distribution, and Hybrid Cryptography offer promising prospects (Amadori et al., 2022).

Yet, before we can look to future solutions, the current issue must be clear. The consequences of the quantum threat could be extreme, but it is unknown how these consequences could play out in more detail. As mentioned in Section 1.4, this research is part of project HAPKIDO, investigating the consequences of quantum unsafe PKI in the scenario where a large quantum computer is in existence. Some work has been published on this topic, although it is not very extensive.

3.5. The societal impact of quantum computing

The three articles of de Wolf (2017), Raban and Hauptman (2018), and Vermaas (2017) are concerned with the effects of quantum computing in general. In 2017, Vermaas wrote an article about the societal impact of quantum computing. In this article, they describe a the potential positive effects of quantum computing through advancements in science. These advancements are expected to happen

because of the increased simulation power quantum computing is expected to hold. They also describe the fact that Shor's algorithm is expected to break current cryptographic standards which are used to secure financial transactions and governmental and company secrets. Furthermore, they describe the changes in cryptographic implementation that are expected to happen to counter the quantum threat. However, this article serves more as a call to societal debate and suggestions on how to do so, rather than an explicit review of the consequences felt by society if the quantum threat to cryptography is not mitigated. In the same issue, de Wolf (2017) elaborates on why the impacts mentioned by Vermaas will happen. However, they also refrain from describing on a detailed level what the societal effects of failing cryptography are. Raban and Hauptman (2018) mention the expected effects of quantum computing on cybersecurity as part of a larger literature review looking into the future of cybersecurity. Again, there is not more detail other than that it is likely to benefit the offensive capabilities in cyberattacks. They do however mention the defensive capabilities of quantum computing in that it offers ways to make communication perfectly secure.

Then there are the studies of Joseph et al. (2022), Mavroeidis et al. (2018), Mulholland et al. (2017), and Yunakovsky et al. (2021) that focus on the quantum threat to cryptography. Of these, Joseph et al. (2022) and Mavroeidis et al. (2018) remain rather general in their mentions of the impact on society that the breaking of asymmetric cryptography by quantum computing has. Additionally, most of their analysis of consequences is rather technical and has little to do with the societal aspects of the technological implementations. Mulholland et al. (2017) and Yunakovsky et al. (2021) are more specific in their discussions of the impacts of the quantum threat. However, both lack the connection to the consequences on a societal level. All of these studies consistently place focus on the technological impacts of the quantum threat. While the technological aspect is important, as it is where societal impact stems from, it should not be forgotten that the real value of technology lies in its implementations in society. This is something that the SRA aims to shed light on.

Lindsay (2020) places the quantum technologies in an international intelligence context and bringing, bringing a new perspective to societal impact. Here, on the one hand is the end of privacy, because of quantum computing breaking cryptography, and on the other the end of intelligence, because of quantum computing securing communications perfectly. Their point however is that history tells us that reality will lie somewhere in between. Alarmists may warn for one or the other end of the spectrum, but the practical and human socio-technical reality in which technology lives renders their arguments void. There are simply too many factors that reduce the effectiveness of cyber offence and defence, also in the face of quantum computing. Even in case of a powerful quantum computer being realised before quantum safe solutions are in place, human organisation and strategic interaction will prevent major shifts in geopolitical balance.

Although no earth-shattering geopolitical weight changes are expected, there is still value in finding the societal risks on a lower (i.e., national, organisational, and individual) level. Not adopting quantum safe technologies will leave societies vulnerable. Lindsay says that the importance of PKI in our societies should not be understated. It is a pillar in online banking, software updates, electronic medical records, virtual private networks & intranets, remote maintenance on industrial machinery, and the monitoring and control of industrial operations, military & governmental access to secure facilities and top-secret information. These applications are confirmed in the other studies in this section. This once more confirms the necessity of this research. Nevertheless, Lindsay's work points out that we should not be fearing the end of the world with the dawn of quantum computing and this notion should be kept in mind when performing the SRA.

Though not specifically investigating the societal risks of the quantum threat, there are two methods

designed to deal with the quantum threat to cryptography. Mosca's XYZ is a simple model to assess the timeline of the quantum threat and provide guidance in when action should be taken (Mosca & Mulholland, 2017). It works by subtracting the shelf life of certain data and the time it takes to implement a quantum safe version of a system from the time it takes until the threat is (estimated to be) actualised. These numbers are of course not meant to be known accurately, but the model does provide a way to think about the threat and the time there is to act. This model only says something about vulnerability, rather than impact.

Another more extensive method is the Cryptography Agility Risk Assessment Framework (CARAF). While it is made not to be specific to the quantum threat, it was designed with the quantum threat as the main example. It includes a component in which the assessor estimates the impact of an expected future threat. However, this is only done on an organisational level and does not reflect the potential influence of the organisation on society. This is where the SRA can fill the gap in the knowledge base. Something of note is that the quantum computing case study in the paper presenting CARAF uses Mosca's XYZ.

3.6. Social / Societal Impact Assessment

When investigating the ways in which societal effects of technology are assessed, the field of Social Impact Assessment (SIA) presented itself. SIA is concerned with identifying and managing social issues arising from planned interventions (Esteves et al., 2012). Quantum computing as a new technology bound to cause disruptions in people's lives seems a good fit for the field. However, in the case of the quantum threat as the object of analysis, there are two issues. Both issues stem from the origins of SIA being project appraisal. The first issue is that SIA is designed to assess the social impacts of a project, meaning the impacts on humans and their interactions, rather than the broader socio-technical impacts. The broader perspective is necessary in face of the quantum threat, because PKI is a prime example of a system in which technology, institutions, and actors coincide.

The second issue is that SIA is founded on the assumption that the analysed development is planned and controllable (Esteves et al., 2012). More specifically, SIA is centred around the implementation of an artefact. This is a problem for the case of the quantum threat, which is not so much an artefact, but rather an imposed threat to security enabled by technological development. Here, the technological development cannot be logically controlled or constrained, as it is sought after all over the world.

In 2015, Wadhwa et al. proposed a SIA-based methodology adapted for security research and security measure implementation. They propose use of the term Societal Impact Assessment, indicating the inclusion of impact on social as well as natural and artefactual systems. This approach solves the first issue discussed above, but the methodology presented by Wadhwa et al. is nonetheless prone to the second issue.

The usage of the term 'societal' and its meaning is a useful takeaway from the SIA field. Moreover, knowing why SIA is not a good fit for analysing the quantum threat brings us closer to what is. A change in perspective that accommodates the fact that the dawn of the quantum threat is imposed rather than a choice is necessary. This is where the concept of risk comes in.

3.7. Risk analysis

While there are many different interpretations of risk in literature (Aven, 2018; Joosten & Smulders, 2014), they share the same two components: values at stake and uncertainties (Aven, 2018). In case of the quantum threat, the many benefits of digital trust and our reliance on it as a society fit in the

first component. As for the second component, the big unknown is when quantum computing will be advanced enough to break current cryptographic standards. This illustrates that when discussing the potential societal effects of the quantum threat to PKI, risk (to society) is a fitting concept. Inspired by Aven (2018) and Wadhwa et al. (2015), this research defines societal risk as the values at stake in human, natural, and artefactual systems; their interactions and the accompanying uncertainty. For the sake of ease, values at stake will be termed impact in the rest of this research.

The separation of risk into the two components of impact and uncertainty is apparent in the SRA. Step 3 establishes the expected impact while step 4 deals with the uncertainty. Both components are part of the eventual risks in step 5.

Before continuing to describe how to find the societal risks, some background on risk as a scientific subject is provided. In 2018, Aven wrote an influential article calling for recognition of Risk Analysis as a distinct science. For Aven, risk analysis encompasses "risk assessment, risk characterisation, risk communication, risk management, and policy relating to risk, in the context of risks that are a concern for individuals, public- and private-sector organisations, and society at a local, regional, national, or global level". Risk analysis is often considered supplemental to other fields. But by comparing risk analysis to statistics, Aven makes the case that risk analysis is in fact a field of its own. Risk analysis and statistics both have limited explanatory power but help greatly in dealing with uncertainties. Knowledge generation in both fields is often highly related to other fields in practical application. For example, statistics are used to inform public policy in curbing a pandemic and risk analysis aids the safe design of a chemical plant. To further conceptualise this, Aven distinguishes between two types of knowledge generation in risk analysis:

- Type A, knowledge related to an activity in the real world, such as the examples given above.
- Type B, knowledge on concepts, theories, frameworks, approaches, principles, methods, and models to understand, assess, characterise, communicate, and (in a broad sense) manage risk.

This ties in with the design science research cycles by Hevner (2007). Type A knowledge generation can be linked to the relevance cycle, whereas type B knowledge generation can be linked to the rigour cycle. The design cycle, residing in the middle (see Figure 2.1), helps to generate both type A and type B knowledge. In this research, the answer to RQ1 is knowledge of type B and the answer to RQ2 is of type A.

One approach to generate type A knowledge recognised by Aven et al. (2018) is predictive analysis. This approach suits the purpose of this research well, as quantum computing and its threat to PKI are future and no similar risks have materialised yet to draw from. When adopting the predictive analysis approach, the following questions are central:

- What will happen if a specific activity is realised?
- What might go wrong?
- Why and how might it go wrong?
- What are the consequences?
- How bad is it?
- What will happen if we (do not) intervene?
- How soon, with what consequences?
- What do we know; what do we not know?
- What are the uncertainties and likelihoods?

The results of a method aiming to uncover the societal risks of the quantum threat should answer these questions.

3.8. Information security risk assessment

To assess the societal risk, a Societal Risk Assessment method (SRA) is necessary. There are many risk assessment (RA) methods available for information security risk. Shamala et al. (2013) describe the shared needs for information in their Information Security Risk Assessment framework. The quantum threat is very much related to information security, as the encryption broken by quantum computing serves it as its main purpose. Another comparative study of information security RA methods was done in 2018 by Wangen et al. They identified three main activities in information security RA: risk identification, risk estimation, and risk evaluation.

The first typically consists of threat, outcome, asset, and vulnerability identification. After these have been identified, the values that go with them are estimated in the risk estimation phase. Lastly, in the risk evaluation phase, the risks are compared and prioritised to finalise the risk assessment process. This provides a basic structure that is proven in practise. Additional to credibility, adopting this basic structure in the SRA promotes two of the design requirements. First, the established information security RA methods were made to be used widely. Basing the SRA on their structure helps the SRA be usable. Second, by adopting a structure that is industry standard, the SRA becomes recognisable. This helps the assessor to understand the use of the SRA more quickly, making the SRA more transferable. The basic structure is adopted as follows: The first phase, risk identification, as recognised by Wangen et al. (2018), is represented by steps 1 and 2 in the SRA. The second phase, risk estimation, is represented by steps 3 and 4. Lastly, the third phase, risk evaluation, is represented by step 5.

Usually in information security RA, threat identification is based on previously identified critical assets (Shamala et al., 2013). CARAF teaches us that when assessing risk related to specific cryptographic vulnerabilities, such as in case of the quantum threat, it is sensible to swap the order. It makes more sense to identify the assets based on the specific cryptographic vulnerability and threat that exploits this vulnerability (Ma et al., 2021). That is why in the SRA, the threats and vulnerabilities are first identified in step 1 and after that, the relevant assets are identified in step 2.

Another lesson from CARAF is that in case of the quantum threat, estimating a probability to capture the uncertainty aspect of risk is not logical. They say that "lack of information about incidents is particularly challenging in the context of crypto agility as the goal is to model the risk of an event that has not yet materialised. For example, let's consider the threat of quantum computing to current cryptosystems. It is not meaningful to consider the frequency of exposure to quantum computing" (Ma et al., 2021, p. 5). Another way to deal with the limited knowledge available on the uncertainty of the quantum threat, is to use Mosca's XZY. This is a simple numerical model which helps to indicate how urgent the risk is. A slightly adapted version is used in step 4 of the SRA.

Wangen et al. (2018) point out that typically, information security RA tends to prioritise technical over organisational aspects. Only one of the eleven compared methods identifies business processes as assets to the organisation. In case of assessing the societal risks of the quantum threat, this is clearly a weakness. It is necessary to widen the scope to be socio-technical, rather than solely technical. Therefore, the SRA incorporates business processes as assets in step 2.

After the comparisons of Shamala et al. (2013) and Wangen et al. (2018), we can conclude that traditional information security RA builds from the bottom up. The risk identification phase is characterised by reasoning from parts (e.g., assets, threats, vulnerabilities, outcomes) to complete scenarios.

This allows for a fine-grained approach that considers many separate but related components. Adopting this structure appeases the highly granular requirement. Starting at this broken down level, the assessor works towards the consequences on a higher, more general level. However, this higher level is limited to the scope of the organisation in traditional information security RA. When aiming to find societal risks, the scope of the organisation needs to be surpassed.

A tried-and-true method that operates on the national level of analysis and assesses risks to national security, i.e., society, is the Integrated Risk Analysis National Security (GRNV) (Analistennetwerk Nationale Veiligheid, 2019). This method has no risk identification phase (or risk evaluation phase). It assumes threat scenarios and initiates the risk estimation phase, in which impacts and likelihood are estimated.

The SRA adds value by combining both approaches above. Leveraging lessons from information security RA practise, risk identification and risk estimation are performed. One information security RA method, Security Risk Assessment Methodology (SecRAM), is particularly useful for its easy-to-use organisational impact estimation (Le Fevre et al., 2017). The organisational impact estimation from SecRAM is used in step 3.2.1 of the SRA. The SRA borrows the organisational impact areas, the organisational impact score matrix, and the confidentiality-integrity-availability structure from SecRAM. Then, to surpass the organisational scope and provide a societal perspective, the GRNV is used in step 3.2.3 of the SRA.

The confidentiality-integrity-availability structure from SecRAM is also applied throughout the rest of the SRA. It uses the three well-established information security properties to categorise different types of information security breaches and the accompanying risks. The properties are defined as follows according to ISO/IEC 27000:2018 (International Organization for Standardization [ISO], 2018):

Confidentiality:	property that information is not made available or disclosed to unauthorised individuals, entities, or processes
Integrity:	property of accuracy and completeness
Availability:	property of being accessible and usable on demand by an authorised entity

By imagining that one of the properties cannot be guaranteed for a certain asset, threat scenarios are imagined. For example, what does it mean when medical dossiers can be seen by unintended third parties (i.e., a breach of confidentiality)? Or when digital financial transactions can be edited by skilled hackers (i.e., a breach of integrity)? Or when pressing charges digitally is not possible anymore (i.e., a breach of availability)? Adopting this structure in the SRA helps the assessor to think in a more granular way, as prescribed by the highly granular requirement.

Table 3.2: Lessons from literature for the SRA

Method/framework	Lesson	Author(s)
Social Impact Analysis Core subjects of risk analysis Risk analysis	Risk rather than impact is the right concept for discussing the expected potential effects of the quantum threat. Risk assessment rather than social impact analysis is field that is suited to the goals of this research.	Esteves et al., 2012 Aven, 2018 Aven et al., 2018
Risk analysis	Risk is composed of impact and uncertainty. These are separately estimated in steps 3 and 4 and combined in step 5 of the SRA.	Aven, 2018
Societal Impact Analysis for security research	When studying societal effects, one should include natural and artefactual systems aside from social systems. This is taken up in my definition of societal risk.	Wadhwa et al., 2015
Information security RA comparisons	Reasoning bottom-up from threats, vulnerabilities, and assets to higher level threat scenarios gives room for a granular approach. The SRA employs this idea throughout its general structure.	Shamala et al., 2013 Wangen et al., 2018
Information security RA completeness framework	Three phases of risk identification, risk estimation, and risk evaluation should be (and are) present in the SRA, making it more usable and transferable.	Wangen et al., 2018
Information security RA completeness framework	Business processes as assets are a useful way to broaden the RA scope to be less technical. This is applied in step 2 of the SRA.	Wangen et al., 2018
CARAF	Asset identification should happen based on the identified threats, rather than the other way around. This is present in the order of steps 1 and 2 in the SRA.	Ma et al., 2021
CARAF	In case of the quantum threat, it makes sense to break with conventional information security RA methods and estimate the uncertainty by using Mosca's XYZ. This is applied in step 4 of the SRA.	Ma et al., 2021
SecRAM	The organisational impact estimation of SecRAM is very straightforward. It is used in step 3.2.1 of the SRA.	Le Fevre et al., 2017
SecRAM	The confidentiality-integrity-availability structure is useful to facilitate granular thinking. It is applied in steps 3, 4, and 5 of the SRA.	Le Fevre et al., 2017

Continued on next page

Table 3.2 – *Continued from previous page*

Method/framework	**Lesson**	**Author(s)**
GRNV	The GRNV provides a way to include a societal impact perspective. It is used in step 3.2.3 of the SRA.	Analistennetwerk Nationale Veiligheid, 2019

4

The Societal Risk Assessment method

In this chapter the Societal Risk Assessment method (SRA) resulting from this research is presented. Many of the elements are taken from existing risk assessment methodology, risk analysis and SIA theory. First, the general purpose of the SRA is laid out. Then, the requirements and their justification. Then, an outline of the method and its components is presented. After that, each individual step is discussed in-depth. Lastly, the application context is explained.

4.1. General purpose

The goal of this method is to capture the most important risks to society that arise from the development of quantum computing in relation to PKI related to an organisation. The goal statement reflects the need to capture risks to society. Therefore, the method is engineered to have the assessing organisation adopt multiple viewpoints and a broad perspective on risk. This desire for a broad perspective has led to the choice to design for use by parties with differing roles in the PKI chain. This means that a policy authority, CA, intermediary CA, end-user, or any other party reliant on PKI usage can make use of the method.

In line with the goal, this method is intended to be used when a party involved with PKI wishes to assess their societal risks considering quantum computing. It helps the assessing organisation achieve a clear understanding of their societal risks, prioritise risks to be treated first, and prepare for transition to quantum safe PKI.

Previous risk assessment methods fall short when it comes to providing a holistic view of the risks of quantum computing to PKI. SecRAM provides a solid general approach to cybersecurity related risk covering many types of impact. Therefore, it provides a solid base for the SRA. However, it is insufficient in two areas. Firstly, it limits its view to consequences to the assessing organisation. This means it is not adequate for assessing the broad notion of societal risk. To broaden the scope and get closer to societal as opposed to organisational risk, the GRNV is introduced. This is a method to assess risks to Dutch national security. The GRNV is designed by the Analyst Network National Security, consisting of prominent knowledge institutes on national security. By making use of the perspective the GRNV provides, the SRA is better able to assess societal risk.

Moreover, SecRAM departs from what an organisation would like to protect (assets) and then derives

vulnerabilities to these assets from existing technologies. This is useful when assessing general cyber risk, but not when there is a need to analyse specific future vulnerabilities. Quantum computing both creates very specific vulnerabilities to specific assets and is a future technology. Therefore, in this case, a different approach is required. This approach is taken by CARAF. It is specifically designed to deal with newly developing technological threats to encryption that create very specific vulnerabilities. Borrowing ideas from CARAF suits the SRA to the quantum threat.

4.2. Requirements

This section describes the requirements that the SRA method is designed for. These requirements are the product of multiple sources of information coming together. The first influence is the goals of HAPKIDO in general and HAPKIDO's work package 1 and by extension the general purpose of the SRA described above. Also, the literature review in Chapter 3 influenced the requirements. Lastly, iterative discussion with both intended users and risk management experts in the user workshops and semi-structured interviews has led to the requirements below.

R1 Usable – Experts across domains should be able to use this method

The SRA should not be limited to a single domain. This is important as PKI and the related societal risks stretch across many domains. Within project HAPKIDO, three domains are represented: eGovernment, banking, and telecom/trust service provision. So, there is a clear link between HAPKIDO's goals and this requirement. Outside of project HAPKIDO, there are many more domains that are affected by the quantum threat in which the SRA could be of use. Therefore, the SRA needs to be designed in a way that accommodates the plurality of domains. This requirement can also be linked to the consistency property from Gregor (2006), because the method needs to be consistent across domains.

R2 Transferable – Domain risk experts should be able to understand and apply this method

This requirement is formed to ensure the applicability of the SRA. The idea, based on the purpose of the method, is to allow for application of the method by field experts and user organisations. This means that the application of the method is not limited to guidance by researchers that are well versed in use of the SRA. However, the requirement is termed transferable, not self-explanatory. Additionally, note the phrasing "domain risk experts…". Both these facts allude to the notion that some guidance and required expertise is acceptable. The reason for this is that the subject matter remains complex to deal with. It is not realistic to expect unguided laymen to effectively use the method. However, efforts should be made to make the SRA as easily transferable as possible. Gregor's (2006) properties simplicity and ease of use are associated with this requirement.

R3 Relevant – Method must include organisational, national, and individual perspectives

An important requirement for the SRA is that its components should be relevant to the goal. The goal is derived from HAPKIDO's work package 1. It should not be like any other information security RA that is scoped to the risks to the assessing organisation. In order for the societal risk assessment to assess societal risks, more than one perspective should be adopted. To get a holistic picture, this research chooses to incorporate three levels of analysis in the SRA: organisational, individual, and national. The quality of results property by Gregor (2006) is connected to this requirement.

R4 Highly granular – Method must facilitate granular description of assets and associated risks

Traditional information RA methods teaches that granular description of assets and elements of risk is very useful. On the one hand, it helps in reasoning forward which risks are run. This is beneficial to the completeness property by Gregor (2006). On the other hand, it helps in reasoning backwards where

certain risks find their source and what effective measures may target. This is beneficial to the quality of results property by Gregor (2006). The highly technical nature of PKI as the source of societal risk is well suited to a highly granular description, as it can be easily divided in components. Of course, there is a trade-off to be made. It makes no sense to keep increasing granularity, as this comes at the cost of the time that it takes to apply the SRA, without adding much benefit. The SRA should facilitate the option for a high granularity, without enforcing it. This way, the assessor can decide the suitable level of granularity that is logical.

4.3. SRA components

To provide a clear overview of the SRA components, IDEF0 modelling is used. This is a suitable tool to model methodologies (Presley & Liles, 1998). The SRA broken down into six steps can be found in Figure 4.1. The activity and purpose of every step can be found in Table 4.1. Each of these steps is thoroughly elaborated upon in the next segment.

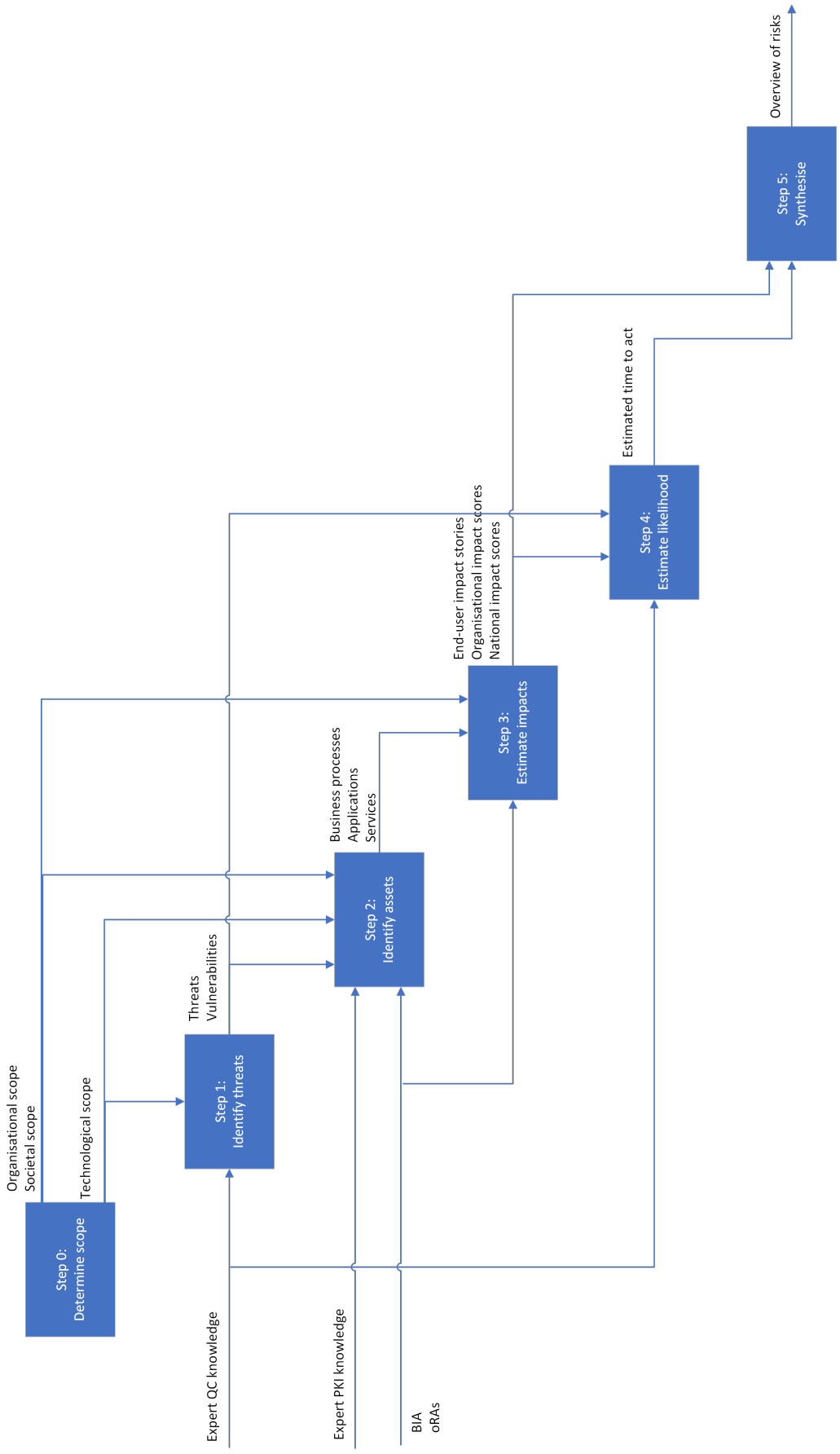

Figure 4.1: SRA A0

Table 4.1: Overview of SRA steps

Step	Activity	Purpose
0: Determine scope	To determine the technological, organisational, and societal influence scope.	To ensure a focussed and highly relevant assessment of risks and avoid wandering.
1: Identify threats	To identify what threats are in scope and what vulnerabilities are exploited by these threats.	To get an idea of what there is to be defended against, so that we may find what to defend.
2: Identify assets	To list the relevant business processes, related PKI applications, and their dependent services.	To have an overview of what is to be defended, so that we may find what is at stake.
3: Estimate impact	To estimate the potential impacts of the threats on the assets from an organisational and a societal perspective.	To give an idea of what is at stake when threats materialise.
4: Estimate likelihood	To review available expert judgement of the estimated time for the threat capacity to exist.	To provide an understanding of how likely certain impact are to occur within a given time.
5: Synthesise	To combine the risk components from the previous steps and rank threat scenarios according to their need to be mitigated.	To generate an overview of the societal risks that the quantum threat brings from the point of view of a single organisation.

As can be seen in Figure 4.2, the output of step 0 is three different scopes to be used in the rest of the SRA: technological, organisational, and societal influence. The technological scope is used to delineate steps 1 and 2, and the organisational and societal influence scopes are used to delineate steps 2 and 3. In step 1, the technological scope is used to inform which threats and vulnerabilities are relevant in the SRA. The threats and vulnerabilities are taken from expert quantum computing knowledge. In step 2, the technological scope is used again to inform which business processes, applications, and services are relevant. These are the three different types of assets used in the SRA. The organisational scope is applied to find the relevant business processes and depending on the assessing organisation also the relevant applications. The applications may also fall within the societal influence scope, as do the services provided. Then, in step 3, the three types of assets are used to find how their compromise could impact the assessing organisation and society. Both the organisational and societal influence scopes are used in this regard. Both the assets and the impacts are assessed by processing a business impact analysis, other previously completed risk assessments, and expert PKI knowledge. Step 4 takes each threat and estimates the corresponding time to act. This estimation is based on expert knowledge of quantum computing and PKI. Now that the organisational and societal impacts and the estimated time per threat is known, they can be combined in step 5 to create an overview of the risks.

4.3.1. Step 0: Determine scope

From NRM we learn that scoping is important in risk management. A scope is seen as "an area which requires a specific type of attention." Good scoping ensures that people can focus their attention on that which matters and avoids discussions that stray from the point (Joosten & Smulders, 2014). Hence, at the start of the SRA, the scope is determined.

An important limitation to the scope of the SRA is technological. In this research, it is only sensible

to limit the scope to quantum computing and its threat to the asymmetric cryptographic basis of PKI. This means that only those things related to quantum computing and PKI should be considered in the SRA. The technological scope could be further specified, depending on the assessing organisation. For example, symmetric cryptography or a distinction between data at-rest, in-transit, or in-use could be considered. Hence, in this step, the assessor is asked to specify the technological scope.

Moreover, it is important that there is a clear distinction between the scope of the organisation and the scope of the influence the organisation has on society. The distinction is illustrated in Figure 4.2. The world of PKI is socio-technical and complex, involving many actors in varying roles that depend on one another to enable services to society. Limiting the scope of analysis to a sole organisation (a) does not do right by this complexity and interdependence. The societal impact cannot be investigated if the assessing organisation does not look further than its own boundaries. On the other hand, broadening the scope to encompass society in its entirety (c) takes away from the specificity to the assessing organisation and thus the usefulness of the SRA to the organisation. As one can imagine, an analysis of how to reduce energy consumption in the Netherlands in general does not provide many actionable focus points to isolating one's house. Therefore, during the SRA, the assessor should walk the line between the scope of the organisation and its influence on society (b). The steps of the SRA are designed to accommodate this. In step 0, the assessor is asked to define an organisational scope and a societal influence scope. As an example, the organisational scope could be limited to a specific branch of the organisation that facilitates or makes use of PKI. The societal influence scope could be geographically limited to the Netherlands. Both scopes are used in the following steps of the SRA. Any scoping decisions can be filled in a table like Table 4.2.

While the scopes considered may seem to be relatively set in stone, there is room for the assessor to further specify wherever deemed necessary. This helps to make the SRA more relevant and thus useful to the assessing organisation. Additionally, this step serves as an exercise to create a better shared understanding among the members of the assessing team of what exactly is to be assessed. This benefits the focus of the assessment and thus the quality of the output.

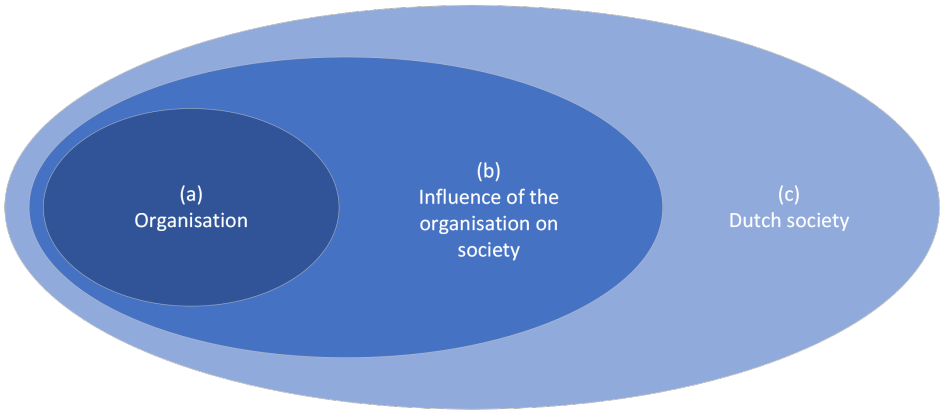

Figure 4.2: Scoping organisational societal influence

4.3.2. Step 1: Identify threats

In step 1, the following question is central: *What to defend against?* This goes against common practice. It is common practice to first identify what is of value and then see what could potentially endanger that. This order of working is common as found by the literature review (Section 3.8). It makes perfect sense when attempting to find what risks in general an organisation is exposed to. However, as CARAF

Table 4.2: Step 0 template

Method/framework	Scope
Technological	The technological scope is limited to • risks that emerge from quantum computing • risks related to PKI • …
Organisational	…
Societal influence	…
Explanation:	

points out, when investigating a specific future technology that poses a threat, it makes more sense to depart from those threats (Ma et al., 2021). The reason is that you may otherwise include many elements in your analysis that are not vulnerable to the specific threat you want to investigate. That is why in the SRA, assessing the threats and vulnerabilities comes first.

The most obvious threat is quantum computing being used to break the security of data real-time, enabling an attacker to spy upon, modify, and interrupt data in-transit, in-use, and at-rest. This threat can be realised once a large enough quantum computer is available. Another threat is that of a store now, decrypt later attack. Such an attack is performed by capturing encrypted data and decrypting it once a powerful enough quantum computer is available. This attack is only relevant to data that needs to remain confidential for longer than the time it takes until a powerful enough quantum computer is available. For example, encrypted medical records that need to remain confidential for 20 years are captured and can be decrypted in 15 years. Such an attack is less powerful than the type described first, but the risk of a store now, decrypt later attack is more immediate. The two threats described are considered the main general threats, but there may be more relevant threats to specific organisations.

The threats are related to vulnerabilities. Vulnerabilities are weaknesses of systems in place that can be exploited to materialise threats. In case of the quantum threat, the reliance of cryptographic security on the factorisation or discrete log problem is a vulnerability. In practice, this means that any reliance on RSA, Diffie-Helmann, or Elliptic Curve Cryptography is a vulnerability. Another vulnerability could be the use of non-doubled symmetric key lengths (because of Grover's algorithm), but only if symmetric cryptography is within the technological scope of the SRA.

During this step, the assessor establishes which threats and vulnerabilities are present and links each threat to a vulnerability. The results can be filled in a table like Table 4.3. The identified vulnerabilities can act as a segue to step 2.

4.3.3. Step 2: Identify assets

Now that we know what is to be defended against from step 1, the next question is *What to defend?*. Finding the answer to this question is necessary to reveal what is at stake. It will be essential in determining the potential impacts of the threats. According to SecRAM, assets are "elements in the system

Table 4.3: Step 1 template

Threat	Vulnerability
Quantum computing breaking asymmetric cryptography real-time 'Store now, decrypt later' tactic capturing sensitive data in-transit protected by PKI …	The use of any cryptographic solution dependent on the discrete log or factorisation problems (e.g., RSA, ECC, DH), which can be broken by quantum computing (i.e., virtually all asymmetric cryptography in place) …

Explanation: ⋯

that have value for the achievement of business objectives or element [*sic*] that support the existence of the business objectives" (Le Fevre et al., 2017, p. 6).

The only assets that are relevant are the ones vulnerable to the threats in scope. Hence, the identified vulnerabilities from step 1 are used to inform the asset identification in step 2.

The SRA defines three different types of assets: business processes, applications, and services. The first, business processes, are "a set of logically related tasks performed to achieve a defined business outcome" (Davenport & Short, 1990, p. 12). These lie within the organisational scope defined in step 0. Keep in mind that any business process, or other asset, included in the SRA should be within the technological scope. This means that every business process should at least have some dependency on or relation to PKI.

After the relevant business processes, the applications are identified. Applications are applications of PKI technology that are reliant on one of the business processes. Applications can be within the organisational scope or only in the societal influence scope. This depends on whether running the full application is a responsibility of the organisation, or the organisation is only responsible for facilitating a part of the application. For example, a CA issuing certificates that are supposed to be used by businesses to automatically authenticate their tax statements is not responsible for the functioning of the application verifying the messages. However, they are responsible for the validity of the certificates used by this application. In this case, the application would be outside of the organisational scope of the CA, but in their societal influence scope.

Lastly, the services dependent on the applications need to be determined. A service is "the execution of information processes provided by an organisation" (N. Bharosa, personal communication, November 1, 2021). Applications in and of themselves are not of value to society. The services they facilitate create societal value and thus the services are a key factor in determining the societal impact if the threats materialise.

All the business processes, applications, and services can be organised in a table such as Table 4.4. Finding any of the assets can be assisted by making use of a pre-existing Business Impact Analysis. Pre-existing risk assessments might be of use as well.

4.3.4. Step 3: Estimate impacts

It is important to note the difference in the impacts of a breach and the impacts of a mitigating measure. In this step, the assessor should stick to the impacts of a breach. Following the definition of risk of

Table 4.4: Step 2 template

Business process Organisational	**Application** Org. / Soc. influence	**Service** Societal influence
		…
	…	…
		…
		…
…	…	…
		…
		…
	…	…
		…

Explanation: ⋯

Aven (2018) explained in the literature review (Section 3.7), impact is an integral part. Therefore, the relevant potential impacts and their gravity need to be estimated. This is done by estimating the impact of compromised assets found in step 2. In information security, there are three properties that can be compromised: confidentiality, integrity, and availability (CIA). The definitions below are taken from ISO/IEC 27000:2018 (International Organization for Standardization [ISO], 2018).

Confidentiality:	property that information is not made available or disclosed to unauthorised individuals, entities, or processes
Integrity:	property of accuracy and completeness
Availability:	property of being accessible and usable on demand by an authorised entity

All impacts are systematically estimated by examining relevant assets combined with a compromised information security property. Additionally, three different perspectives with differing impact areas are considered. These are the organisational perspective, related to the organisational scope, and the end-user and national perspectives, related to the societal influence scope. All three perspectives are separately adopted, starting with the organisational perspective.

Step 3.1: Estimate organisational impacts

When assessing the impact from an organisational perspective, it is important to keep the organisational scope in mind. This means that the business processes defined in step 2 are the assets to be considered, as they fall within the organisational scope. In assessing the organisational impact, SecRAM provides guidance. As in SecRAM, every asset is judged on a compromised information security property. SecRAM prescribes seven different impact areas to be considered when assessing the impact. These are personnel, capacity, performance, economic, branding, regulatory, and environment. Every combination of business process, CIA property, and impact area is given an impact score from A to E.

These scores can be filled in Table 4.6. To determine which score should be given, a score card such as Table 4.7 can be used. The score card presented here is an example, it can be adapted as deemed necessary. After every combination is scored, the highest score of each row should be copied to the 'Total' column. This reduces the organisational impact to a single score per CIA property per business process.

Table 4.6: Step 3.1 template

Business process	**CIA**	**Personnel**	**Capacity**	**Performance**	**Economic**	**Branding**	**Regulatory**	**Environment**	**Total**
	C	…	…	…	…	…	…	…	…
…	I	…	…	…	…	…	…	…	…
	A	…	…	…	…	…	…	…	…
	C	…	…	…	…	…	…	…	…
…	I	…	…	…	…	…	…	…	…
	A	…	…	…	…	…	…	…	…

Explanation: …

Table 4.7: Organisational impact score card taken from SecRAM (Le Fevre et al., 2017)

Impact Areas	A No impact	B Minor	C Severe	D Critical	E Catastrophic
Personnel	No injuries	Minor injuries	Severe injuries	Multiple severe injuries	Fatalities
Capacity	No capacity loss	Loss of up to 10% capacity	Loss of 10% - 30% capacity	Loss of 30% - 60% capacity	Loss of 60% - 100% capacity
Performance	No quality abuse	Minor system quality abuse	Severe quality abuse that makes systems partially inoperable	Major quality abuse that makes major system inoperable	Major quality abuse that makes multiple major systems inoperable
Economic	No effect	Minor loss of income	Large loss of income	Serious loss of income	Bankruptcy or loss of all income
Branding	No impact	Minor complaints	Complaints and local attention	National attention	Government & international attention
Regulatory	No impact	Minor regulatory infraction	Multiple minor regulatory infractions	Major regulatory infraction	Multiple major regulatory infractions
Environment	Insignificant	Short term impact on environment	Severe pollution with noticeable impact on environment	Severe pollution with long term impact on environment	Widespread or catastrophic impact on environment

Step 3.2: Estimate societal impacts
After the organisational impacts are estimated, the assessor moves on to the societal impacts. For this part, the societal influence scope is leading instead of the organisational scope (Figure 4.2). Estimating the organisational impact is done for every business process. Every business process is associated with at least one, but likely multiple services. To estimate the potential societal impacts, the services are the assets to judge. The societal impact of each business process is decided by the societal impact of its related services.

Step 3.2.1: Estimate end-user impacts Estimating the societal impacts per business process is done in two steps. First, the end-user perspective is adopted. The assessor estimates what effects the end-user of a service of an application would feel in case of a compromise. This produces a few sentences of written text for every application/CIA property combination, as can be filled in Table 4.8. Taking this step is necessary to force the assessor to think about the impact that a compromise within the scope of their organisation may have on individuals outside of that scope. It is easier to think of how an individual may be impacted than to come up with ideas how the whole of society may be impacted. This intermediary step serves as a bridge to help think of impacts for the whole of society.

Table 4.8: Step 3.2.1 template

Business process	⋯	
Application	**CIA**	**Consequences for end-users**
⋯	C	⋯
	I	⋯
	A	⋯
⋯	C	⋯
	I	⋯
	A	⋯

Explanation: ⋯

Step 3.2.2: Estimate national impacts The next step in estimating the societal impact is taking on a national perspective and giving corresponding impact scores. To do so, the GRNV is consulted. It is specifically designed to assess disrupting effects to society on a national level from a security point of view. This method is used to inform the national security strategy of the Dutch government (TNO, n.d.).

Similar to the way the organisational impact is scored, the societal impact is scored. The impact areas in Table 4.10 taken from SecRAM are replaced by impact areas from GRNV. Some impact areas from GRNV are deemed more relevant than others. Although not all impact areas will be applicable, all should be considered so that no kind of impact will go unnoticed. The full list of impact areas with the more relevant ones in bold can be found in Table 4.9.

To determine the scores for each impact area, the GRNV is applied. For every impact area, the GRNV describes how to determine the (societal) impact score. The threat scenario that is considered is that a

Table 4.9: Societal impact areas (Analistennetwerk Nationale Veiligheid, 2019)

National security concern	Impact area
1. Territorial security	1.1 Violation of the integrity of (Dutch) soil
	1.2 Violation of the integrity of the international position of the Netherlands
	1.3 Violation of the integrity of cyberspace
	1.4 Violation of the integrity of allied soil
2. Physical security	2.1 Deaths
	2.2 Seriously injured and chronically sick
	2.3 Lack of basic needs
3. Economic security	3.1 Costs
	3.2 Degradation of the vitality of the Dutch economy
4. Ecological security	4.1 Long-lasting damage to nature and the environment
5. Social and political stability	5.1 Disruption of day-to-day life
	5.2 Degradation of the democratic rule of law
	5.3 Societal unrest
6. International rule of law	6.1 Degradation of the norms of state sovereignty, peaceful co-existence, and peaceful conflict resolution
	6.2 Degradation of the working, legitimacy or compliance with international treaties and norms concerning human rights
	6.3 Degradation of a rule-based international financial-economic order
	6.4 Degradation of the effectiveness and legitimacy of multilateral institutions

certain type of compromise (CIA) occurs affecting all services of all applications dependent on a certain business process. This is repeated for every business process. The scores are taken up in Table 4.10. To estimate the impacts, deep knowledge about the business processes is necessary. Additionally, organisations can make use of business impact analyses and previously done risk assessments.

4.3.5. Step 4: Estimate likelihood

As defined earlier, societal risk has two parts. The previous steps have dealt with the value at stake. This step deals with the uncertainty. The quantum threat is a future threat of which there has not been a materialised instance. Because of this, traditional approaches designed to deal with present threats are not applicable. Therefore, this SRA takes on Mosca's XYZ model, which determines how much time there is left to act (Mosca & Mulholland, 2017). As this time to act is based on assumptions, it serves as an approximation and a way to use available knowledge to deal with uncertainty. The variables of Mosca's model are defined as follows:

Table 4.10: Step 3.2.2 template

Business process	CIA	1.2 International position	1.3 Cyberspace	3.1 Costs	3.2 Economy	5.1 Day-to-day life	5.2 Rule of law	⋮	Total
	C	…	…	…	…	…	…	…	…
…	I	…	…	…	…	…	…	…	…
	A	…	…	…	…	…	…	…	…
	C	…	…	…	…	…	…	…	…
…	I	…	…	…	…	…	…	…	…
	A	…	…	…	…	…	…	…	…

Explanation: …

X = longest shelf life of data within the scope of the business process [years]

Y = time it will take to replace all vulnerable cryptography used within the scope of the business process to quantum safe cryptography [years]

Z = estimated time until a powerful enough quantum computer is available [years] (may vary depending on risk appetite)

The estimated variables and the theoretical time to act (t) are to be filled in Table 4.11. The formula for t is based on the threat. Do note that t is an approximation, not an exact prediction.

4.3.6. Step 5: Synthesise

In this step, all work of previous steps is combined. This results in a priority list of business processes to secure first. The high scoring business processes can be traced back in previous steps, to see where the high scores originate from. This gives insight in the internal dependencies of the SRA.

The results from all previous steps are combined in a single table like Table 4.12. The organisational and national impact are taken from Steps 3.1 and 3.2.2 respectively. The theoretical time to act (t) is taken from Step 4. Lastly, using the conversion matrix (Table 4.13), the risks can be ranked. Taking the highest of the two impact scores and the theoretical time to act, the matrix ranks the risk for each threat to each business process. Table 4.14 presents the aggregated results. It should be noted that the conversion matrix can be adjusted according to the risk appetite of the assessing organisation.

Table 4.11: Step 4 template

Business process	*X*	*Y*	*Z*	**Threat**	**Formula for *t***	*t*
…	…	…	…	Real-time access (CIA)	t = Z – Y	⋯
				Store now, decrypt later (C)	t = Z – X – Y	⋯
…	…	…	…	Real-time access (CIA)	t = Z – Y	⋯
				Store now, decrypt later (C)	t = Z – X – Y	⋯
…	…	…	…	Real-time access (CIA)	t = Z – Y	⋯
				Store now, decrypt later (C)	t = Z – X – Y	⋯
…	…	…	…	Real-time access (CIA)	t = Z – Y	⋯
				Store now, decrypt later (C)	t = Z – X – Y	⋯

Explanation: ⋯

Table 4.12: Step 5 overview template

Business process	**Threat**	**Organisational impact**	**National impact**	*t*
…	Real-time access (CIA)	⋯	⋯	⋯
	Store now, decrypt later (C)	⋯	⋯	⋯
…	Real-time access (CIA)	⋯	⋯	⋯
	Store now, decrypt later (C)	⋯	⋯	⋯
…	Real-time access (CIA)	⋯	⋯	⋯
	Store now, decrypt later (C)	⋯	⋯	⋯
…	Real-time access (CIA)	⋯	⋯	⋯
	Store now, decrypt later (C)	⋯	⋯	⋯

Explanation: ⋯

Table 4.13: Step 5 conversion matrix example

Impact score	t			
	> 5	$4 - 0$	$-1 - -5$	< -5
A	Acceptable	Acceptable	Moderate	Moderate
B	Acceptable	Acceptable	Moderate	Severe
C	Acceptable	Moderate	Severe	Severe
D	Moderate	Severe	Severe	Critical
E	Severe	Severe	Critical	Critical

Table 4.14: Step 5 synthesis results template

Business process	**Threat**	**Risk category**
…	Real-time access (CIA)	⋯
	Store now, decrypt later (C)	⋯
…	Real-time access (CIA)	⋯
	Store now, decrypt later (C)	⋯
…	Real-time access (CIA)	⋯
	Store now, decrypt later (C)	⋯
…	Real-time access (CIA)	⋯
	Store now, decrypt later (C)	⋯
Explanation: ⋯		

4.3.7. SRA output

An important part of the SRA is how the output is handled afterwards. The SRA is not complete without a report detailing the particularities encountered during the assessment and what they mean for the results and any potential next steps in mitigation. This report should be like a management summary for the SRA complete with conclusions and recommendations.

4.4. Application context

The SRA is a method, a tool that needs to be applied. Without proper application, it cannot be effective. Imagine a hammer gripped by the head instead of the handle, thrust instead of swung, or held by a person not strong enough. All of these ways of handling the tool render its use not as effective as it can be. This is why the application context matters. Just like the hammer, the SRA benefits from proper application. This starts with who is intended to use to SRA.

4.4.1. Who should apply the SRA?

As mentioned in Section 4.1, the SRA is intended to be used by a wide variety of actors. But, the SRA is not meant to be used by just any- and everybody. The organisation from whose viewpoint the SRA is applied is called the assessing organisation. The assessing organisation should in some way be reliant on PKI. This may be through activities in trust service provision in varying roles such as policy authority, registration authority, root CA, or intermediary CA. It could also be through the use of leaf certificates to gain access to trust services or being reliant on the use of leaf certificates by other parties. As the building blocks of the SRA are inspired by general information security RAs, the SRA is not domain specific. That means that the assessing organisation can come from any domain, so long as the organisation is reliant on PKI somehow. The assessing organisation should also be interested in knowing the risks they run in a societal context and/or doing business in a socially responsible manner. These parties can use the knowledge gained from the SRA to take action or changing their policies on becoming quantum safe.

With this user group in mind, the SRA was designed. This resulted in the choice to limit the scope to the viewpoint of the assessing organisation and their influence on society, rather than the composite influence on society of multiple organisations. This choice was made because of three reasons. First, it provides an incentive for organisation to perform the SRA. It allows organisations to get insights relevant to them. They get to see their risks and their influence on society. Second, the assessment will be less complicated as no multiple viewpoints clash and clutter the analysis. Third, it is easier to organise a session within an organisation than with people from multiple organisations.

However, there is a drawback to this scoping choice. There is less detailed oversight on the actual societal risks. The chained nature of hierarchical trust present in PKI creates dependencies outside of the view of the assessing organisation. For example, Logius as the policy authority of PKIoverheid is not fully aware of all exact use cases in practice of all certificates under their umbrella infrastructure. This information resides with parties lower in the trust chain that manage applications dependent on PKIoverheid certificates (A. de Ruiter, personal communication, February 24, 2022).

To overcome this drawback, publicly motivated research projects (e.g., HAPKIDO) or other collaborations can combine insights of SRAs done by multiple organisations. This way, knowledge from the entire trust chain, top to bottom, and in multiple sectors can be leveraged and the societal risks can be accurately and widely assessed. It is the task of such projects and collaborations to decide how much detail needs to be known in order to paint an adequate picture of the societal risk. Apart from which organisation is to perform the SRA, it also matters who inside the organisation is present during the actual performance of the SRA. As this is a more practical question, it is discussed in the next section.

4.4.2. How to apply the SRA?

As an organisation, there are a multitude of ways in which tools such as the SRA can be applied. In the case of the SRA, we first take a look at what kind of people should be involved during the SRA. This group of people is called the assessor. Ideally, there is a mix of expertise present. Risk assessment in general thrives on diversity of expertise (M. Klaver, personal communication, December 21, 2021). In case of the SRA, it is advised to have at least one expert present on the following knowledge areas: risk management, (senior) management, technology (i.e., PKI), potentially affected business processes, and compliance. Additionally, while in-depth knowledge of quantum computing is not necessary, it is strongly recommended to have some shared knowledge on how quantum computing affects PKI. In-house experts are necessary, as (tacit) knowledge of the assessing organisation is necessary. Yet, not all experts need to be in-house. External experts can be a great addition. It should be noted that the

composition of the assessor is based on expert consultation and is not rigorously researched.

Another aspect of the way in which the SRA is applied, is the depth of analysis. Because of the high granularity requirement, the SRA facilitates a deep analysis. However, per case it is applied to, the required depth of analysis may vary. It is the task of the assessor to attain the right depth of analysis for the case. This is done in multiple steps of the SRA. Steps 0, 1, particularly 2, but also 3 are where the depth is decided. In step 0, the scoping can be described in a very broad and general way, or it can be made very specific. The same goes for the threats and vulnerabilities in step 1. In step 2, the assets can be categorised in a fine-grained way, or in brush strokes. For example, a business process can be described as broad as "safeguarding digital trust in our PKI" or as narrow as "assisting our customers of service X with certificate renewal". Similarly, an application could be Digipoort as a whole, or a specific part of Digipoort. As for the dependent services, one could be described as tax reporting in general or reporting a specific kind of tax by a specific kind of party. Taking a deep and granular approach may benefit the output of the SRA, but it takes longer to do the assessment. Of course, at a certain point, it may take much more time to be more specific, while it is marginally beneficial to the output. Hence, the trade-off between granularity/depth and time to complete the assessment.

So, the time it takes to perform the SRA is dependent on the depth of analysis. Ideally, the SRA should be completed in a single session, so that the assessment remains focused. Comparable RAs take a single session of between four to six hours to be completed (M. Klaver, personal communication, December 21, 2021). Based on the speed of the user workshops and the evaluation session, this seems realistic. However, this has not been properly tested. The time necessary is also dependent on the efficiency of the session. This is reliant on proper guidance of the assessor.

Proper guidance of the assessor is important for the efficiency of the session and the quality of the SRA output. For example, improper guidance can lead to vague scoping. Here, participants will keep adding information to the discussion which may not be as relevant to the assessment as they think. It could lead to participants talking about differing concepts without realising that they are. This muddies the analysis and takes up time and mental space. This problem is common in risk management practice (A. Smulders, personal communication, January 26, 2022). Good guidance can curb such and other behaviours distracting from a focused assessment. There are several ways in which guidance can be offered. One of which is the provision of a manual. The SRA template in Appendix A is a good starting point, but for a good manual there needs to be more introductory and conclusive text. Another option is a tutorial video or workshop to be followed beforehand. This is a good way to more actively show the purpose and workings of the SRA. To add to this, an exemplary case can provide a means to make the abstractions of the SRA concrete. These three options can be provided in conjunction to maximise their effect. Lastly, a session leader should be appointed to guide the assessment. This leader should be well-aware of the guidance materials and preferable have pre-existing knowledge of risk management. The guidance options are directly related to the transferable requirement.

A more practical concern is tooling. For this research, the use of Word documents and online collaborative word processing documents was sufficient. However, this was at times awkward because of the need for flexible table editing and tables being cut off due to page sizes. A better workflow would be enabled if a tool specific for the purpose of applying the SRA was made. This could be a webtool which runs client-side to avoid issues with sensitive data, as it would be easily accessible to users. On the other hand, because very sensitive information about business vulnerabilities is being handled, users may prefer to stay away from a browser communicating with the open internet altogether. In this case, a portable open source program would be the better choice.

4.4.3. Concluding remarks

The following statements summarise the application context and ideas that the SRA is based on:

- The SRA can be applied by any party that is reliant on PKI and wants to know the risks they run in a societal context because of their PKI reliance.
- The SRA is designed to be domain unspecific and is expected to work similarly across domains.
- It is advised to perform the assessment with a team of experts with expertise in risk management, (senior) management, technology (i.e., PKI), potentially affected business processes, and compliance.
- It is advised that the assessment is guided by an assessment leader that is acquainted with the SRA method.
- The assessment is expected to take four to six hours.
- A report should be drawn up from the results of the assessment to maximise actionable insights.

4.5. Evaluation

After every user workshop, feedback was structured in SWOT analyses by listening back to the recordings of the workshops. These SWOT analyses are documented in Appendix B. In the output evaluation workshop, the participants were asked to collaboratively fill in a SWOT analysis themselves. The results of all SWOT analyses have been combined in Table 4.15. In the following section, the SRA is evaluated per requirement.

4.5.1. Evaluation per requirement

Each strength, weakness, opportunity, and threat is related to one or more requirements. These are discussed below per requirement, starting with the usable requirement.

R1 **Usable – Experts across domains should be able to use this method**

To be clear, this requirement is about how well users across domains are able to apply the method, given that they have no problems understanding how the method is supposed to be applied. The following weaknesses and threats identified by the participants of the user workshops indicate that the SRA is not an assessment that can be quickly banged out. It is clear that a lot of knowledge and thought is required. This emphasises the need for a wide variety of experts during the assessment. Although the SRA may be perceived as lengthy, I consider this a necessary evil. It is simply quite a complex topic, which means it requires some time to figure out. There is an opportunity that may be leveraged to improve the usability of the SRA, by providing access to clear and already processed information ready to be used in the SRA. Documents that are often in existence by good business practice can offer valuable input. These documents are business impact analyses and previously done risk assessments as part of business continuity planning.

W Requires a lot of knowledge on business processes

W Risk assessment is a tough process for business owners

W Information with the required level of detail can be hard to find

T The likelihood is very hard to properly assess

T Can be perceived as lengthy (and complex)

O Documents such as a Business Impact Analyses and previously done can be valuable input

Table 4.15: Combined SWOT analysis of the SRA

Strengths	**Weaknesses**
• This method addresses the recognised need for insight into societal risks because of the quantum threat to PKI • The method feels familiar to those with some experience in risk assessment • The multiple perspectives on impact assessment • The step-by-step nature enables 'peeling off' the different layers and provides granularity and insight in dependencies	• Does not distinguish between threat actors • Does not include mitigation risks • Requires a lot of knowledge on business processes • Information with the required level of detail can be hard to find • Risk assessment is a tough process for business owners • Difficult to pull mitigation strategies from
Opportunities	**Threats**
• Documents such as a Business Impact Analyses and previously done risk assessments can be valuable input • Present the SRA as a self-assessment and combine the results with recommendations/action pathways	• The likelihood is very hard to properly assess • Organisational impact: capacity & performance may be differently interpreted by different assessing parties, depending on their industry • Parties are not likely to share sensitive information about their perceived vulnerabilities such as a Business Impact Analysis and previously done risk assessments • Can be perceived as lengthy and complex • Lack of clarity about the need for extensive insights

The following threat and opportunity are linked. The problem that parties are not willing to share sensitive information may be alleviated by having the SRA be a self-assessment in which the sensitive information can be kept to the assessing organisation. By combining the results of the SRA with recommendations/action pathways, the assessing organisation can effectively use the results without ever needing external help. This is something to be further researched by combining work package 1 with other work packages from project HAPKIDO.

T Parties are not likely to share sensitive information about their perceived vulnerabilities such as a Business Impact Analysis and previously done risk assessments

O Present the SRA as a self-assessment and combine the results with recommendations/action pathways

In conclusion, the combined SWOT points towards some problems with usability in the sense that it may be hard for some users and requires effort. This may be helped somewhat in future versions of the SRA. On the other hand, it will always require effort to do the SRA, as the topic itself remains complex. In terms of usability across domains, no weaknesses or threats were identified. This seems to be a good thing.

R2 **Transferable – Domain risk experts should be able to understand and apply this method**

This requirement is about how well users understand how to apply the SRA. As it turns out, the use of existing information security RA structures and building blocks has paid off. Because of the familiarity, the method is more easily understood. However, it can still seem complex and lacking clarity about why the granularity is necessary. These threats can be taken on by applying the advice on guidance presented in Section 4.4.2.

S The method feels familiar to those with some experience in risk assessment

T Can be perceived as (lengthy and) complex

T Lack of clarity about the need for extensive insights

One identified weakness was about the potential for some concepts to be understood differently by differing assessing organisations. This may also be taken on by applying the guidance advice from Section 4.4.2. But, it should be noted that this may not be an issue per se. In the end, risk assessment is subjective. The meaning of the scores and filled in answers is what the assessor assigns to them. The results of the SRA are still valid, as they are relevant to the assessing organisation according to the assessor.

W Organisational impact: capacity & performance may be differently interpreted by different assessing parties, depending on their industry

Summarising, the transferability seems to be not perfect, but not too bad either. With some additional work on guidance, the transferability can be improved.

R3 **Relevant – Method must include organisational, national, and individual perspectives**

Both strengths identified below can be linked to the relevancy of the SRA. Many of the participants indicated their interest in the SRA and that the goals of the method are relevant. Moreover, the multi-perspective approach is seen as a plus.

S This method addresses the recognised need for insight into societal risks because of the quantum threat to PKI

S The multiple perspectives on impact assessment

However, the limited scope of the SRA focusing on the risks of quantum unsafe PKI in the quantum era was less well-received. Some participants would rather have a method that includes the risks involved with mitigation of the quantum threat. This is outside of the scope of work package 1 of project HAPKIDO, for which this SRA was developed. This should be taken as a sign that participants are in fact interested in seeing the risks that come with handling the quantum threat as well and thus it should be seen as a stimulus for the rest of project HAPKIDO.

W Does not include mitigation risks

W Difficult to pull mitigation strategies from

In short, the SRA is relevant. Where it falls short is because of the explicit scoping choice to fit in project HAPKIDO's work package 1. This should be taken up in the other work packages of HAPKIDO.

R4 **Highly granular – Method must facilitate granular description of assets and associated risks**

The strength identified signals that the SRA is deemed to be granular and at the right level of detail to be useful. One slight comment on that is that there is no distinction between threat actors. This allows for less granularity of the threat scenarios. Yet, this was a deliberate choice, as most participants did not view the distinction to add much value to the assessment, but it does complicate the assessment.

S The step-by-step nature enables 'peeling off' the different layers and provides granularity and insight in dependencies

W Does not distinguish between threat actors

One weakness that might take away from the granularity of the assessment is that highly granular information can be hard to find. Unfortunately, this is something that cannot be dealt with from the SRA development side. The information resides with the users and after all, the output of any method can only be as good as its input.

W Information with the required level of detail can be hard to find

To conclude, the SRA is a granular method. This benefits the results. Not always can the SRA be implemented as granular as the method allows, as highly detailed information may be hard or even impossible to find.

4.5.2. Concluding remarks

Overall, the combined SWOT reflects two main beliefs about the SRA among experts. Firstly, the SRA serves a relevant purpose, is of value, and achieves its goal. The second belief is that the SRA is somewhat complex, requires deep knowledge of business processes which might be hard to find, and asks for experience with risk assessment. To help ease the problems that come with the second belief, guidance should be offered and business impact analyses and previously completed risk assessments can be used as input. However, these input documents may be hard to gain access to as well, as they are often confidential.

5

Case study: Logius, Policy Authority of PKIoverheid

In this chapter, the SRA is applied to the case of Logius as the Policy Authority of PKIoverheid. This is done with two goals in mind. The first goal is to evaluate the SRA as the outcome of the design process. Evaluation of the artefact is necessary in good design science research and doing a case study is one of the ways to achieve that (Hevner et al., 2004). The second goal is to gain insight into the societal risks that the quantum threat poses to PKI. By doing an instrumental case study, I am not solely interested in the specifics of the eGovernment case, but also in insights that may be applicable to other domains as well (Stake, 2003).

5.1. Case description

PKIoverheid (PKIo) is a transparent trust framework that provides security for communication between government and government, government and business, business and business, and government and citizen (Logius, 2022). It is managed by Logius, on behalf of the Ministry of Interior and Kingdom Relations. It was set up to accommodate the need for digital trust, which came with the shift towards electronic transactions.

PKIoverheid is built in such a way that the the central level and the operating level are separated. The operating level is where the TSPs interact with the end-users directly. The central level is split into domains based on roles. For the publicly trusted root, these domains are Organisation Person, Organisation Services, Citizen, and Autonomous Devices. There is also a private root that issues certificates that are not publicly trusted. The private root has the domains Private Services and Private Persons. Each domain has its own CA certificate, signed by the corresponding root CA. This division of domains provides transparency about the role fulfilled in the digital transaction by the certificate user. Additionally, by splitting the certificates based on roles, different security criteria can be used in supplying the certificates.

Each domain CA certificate is used to sign domain specific issuing CA certificates that are managed by TSPs. The TSPs use their issuing CA certificates to issue certificates to end-users. Table 5.1 describes all PKIoverheid TSPs, the domains in which they are active, and whether they are commercially active. The non-commercial TSPs provide certificates for specific applications. Most commercial TSPs offer a

Table 5.1: Overview of PKIoverheid TSPs

TSP	Domain(s)	Commercial
Cleverbase	Citizen	Yes
Digidentity	Organisation Person, Organisation Services, Citizen, Private Services	Yes
Healthcare Insurance Provider Identification and Authentication Register (ZOVAR)	Private Services	No
KPN	Organisation Person, Organisation Services, Private Services	Yes
Ministry of Defence	Organisation Person	No
Ministry of Infrastructure and Water Management	Organisation Person, Organisation Services, Autonomous Devices	No
QuoVadis	Organisation Person, Organisation Services, Citizen, Private Person, Private Services	Yes
Unique Healthcare Provider Identification Register (UZI-register)	Organisation Person, Organisation Services, Private Services	No

wide selection of certificates for many use-cases. Hence, the large amount of domains in which they are active. Cleverbase is the exception, as it issues certificates for a specific application: identification and signing by citizens through Vidua.

Logius is the Policy Authority of PKIoverheid. As the Policy Authority, Logius has the following tasks listed in their Programme of Requirements (2022, p. 5):

1. contributing towards the development and the maintenance of the framework of standards that underlies the government's PKI, the Programme of Requirements (PoR);
2. supervising and preparing for the process of admittance of Trust Service Providers (TSPs) to the government's PKI;
3. regulating and monitoring the activities of TSPs that issue certificates under the root of the government's PKI

Essentially, Logius is tasked with regulating the use of PKIoverheid through the Programme of Requirements; regulating and executing the admittance of new TSPs; and checking compliance of participating TSPs with the Programme of Requirements. This means that while TSPs execute the issuing of leaf certificates and take liability for this, Logius is responsible for the functioning and trustworthiness of PKIoverheid as a whole. The controls Logius employs to fulfil this responsibility are described in Logius' certificate practice statement. Logius' controls are in some ways more strict than the highest level of security defined in eIDAS (A. de Ruiter, personal communication, February 24, 2022).

Because of the split in the central part and the operating part of PKIoverheid, Logius does not have complete oversight of leaf certificates and their use. Logius simply is not responsible for managing this, the TSPs are. This means that Logius' view on societal impact is obscured. Therefore, it is all the more interesting to apply the SRA to this case and see how well it serves to assess the societal risks.

Another limitation in this case study is that Logius' Business Impact Analysis (BIA) is classified and can thus not be used in this research. (Internal) Access to this BIA and other previously completed risk

Table 5.2: Overview of risks in case study

Business process	Threat	Risk category
Trustworthiness assurance of the Organisation Person Domain	Real-time access (CIA)	Severe
	Store now, decrypt later (C)	Critical
Trustworthiness assurance of the Organisation Services Domain	Real-time access (CIA)	Severe
	Store now, decrypt later (C)	Critical
Trustworthiness assurance of the Citizen Domain	Real-time access (CIA)	Moderate
	Store now, decrypt later (C)	Critical
Trustworthiness assurance of the Autonomous Devices Domain	Real-time access (CIA)	Moderate
	Store now, decrypt later (C)	Severe
Trustworthiness assurance of the public root CA	Real-time access (CIA)	Severe
	Store now, decrypt later (C)	Critical
Trustworthiness assurance of the Private Services Domain	Real-time access (CIA)	Severe
	Store now, decrypt later (C)	Severe

assessments could further improve the accuracy of the results.

5.2. Case results

The final overview of risks as the output of the applied SRA is presented in Table 5.2. This is only a very concentrated end product of the assessment. For the full picture and how these risks were derived, see the fully applied SRA documented in Appendix C. The results of this full application are summarised below.

First of all, it should be noted that the validation of the results was done rather quickly and by a small group of experts. More time should be invested in thoroughly validating the results, before the conclusions can be considered final.

Logius has divided its PKIoverheid architecture in several root CAs and domain CAs. The assurance of the trustworthiness of each of these domains and the root CAs are the main assets in the assessment. Overall, it becomes clear that the societal risks of the quantum threat from Logius' perspective are fairly high. The risks are the worst from an organisational point of view, especially considering store now, decrypt later attacks. These attacks may lead to loss of confidentiality for very sensitive data and there is little time to act. When looking at Table 5.2, the conclusion is that Logius should move quickly to secure the applications that use the most sensitive data first as a defence against store now, decrypt later attacks. These are in the Organisation Person, Organisation Services, and Citizen domains. Naturally, the public root CA above these domains needs to be secured as well.

The risks for Logius are so high because of the wide impact that breaches in trustworthiness assurance of PKIoverheid has. PKIoverheid is used in many applications throughout Dutch society and is the main support of communication with the Dutch government by citizens and organisations. The assessment shows how widespread in society this dependency is.

The shelf life of highly sensitive information such as medical history, political preference, and religion is assumed to be twenty years. One could argue that this information should stay confidential as long

Table 5.3: SRA output evaluation statements

Statement	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
1. The SRA gives a complete picture of the relevant risks					2	2	
2. The SRA provides the right level of granularity			1			3	
3. The SRA is simple to understand			1	1	2		
4. The SRA is easy to use			2		2		
5. People need help using this SRA						4	
6. The SRA produces actionable insights					3	1	
7. I would recommend this SRA to colleagues				1		2	1

as the data subject is alive or even after. Without this assumption of personal data shelf life, Logius is already too late to prevent loss of confidentiality of sensitive data.

The criteria used to determine societal impact on day-to-day life in the GRNV point to no significant impact. However, when examining the individual end-user impacts, it is abundantly clear that citizens will feel the effects of PKIoverheid failing in their day-to-day life.

There are a myriad of ways in which society may be impacted if Logius is not able to secure PKIoverheid. Examples include interference with information exchange for medical professionals; leaking of company secrets of many companies operating in the Netherlands; potential loss of any application that uses DigiD facilitating communication between the Dutch government and citizens; large scale fraud because accountants, bailiffs, and notaries cannot securely sign documents; and leaking of military intelligence, as secure communications are very hard to set up.

5.3. Evaluation of output

In the evaluation workshop, the four participants were asked to evaluate the SRA and its output given a few statements. The statements are based on the evaluation criteria for methods by Gregor (2006) and adapted to better suit the SRA context. This is explained in Section 2.5. It should be noted that this enquiry was done with only four respondents. The evaluation of the SRA is indicative, not conclusive. The results can be found in Table 5.3.

When comparing these results with the origin of the statements from Gregor's evaluation criteria for methods in Table 2.2, we see the following results. The results seem to indicate that the quality of results from the SRA is quite alright (statements 2 and 6). The same holds true for the completeness of the method (statement 1). The SRA performs less well for the criteria ease of use and simplicity (statements 3, 4, and 5).

These statements and the general comments during the evaluation workshop can be related to the

design requirements. This is done below, starting with the usable requirement.

R1 Usable – Experts across domains should be able to use this method

When looking at statement 4, the evaluation scores indicate that the SRA is usable, but its usability is not great. This is in agreement with the comments during the output evaluation workshop. It seems that there is a need for hard to gain information and gathering the experts with this knowledge is not an easy task. This should be kept in mind when preparing to use the SRA.

R2 Transferable – Domain risk experts should be able to understand and apply this method

A clear finding in the evaluation workshop is that there is a need for guidance during the SRA. The responses to statements 3 and 5 are also indicative of this need. This means that the SRA as-is, without such guidance, is not as transferable as it should be.

R3 Relevant – Method must include organisational, national, and individual perspectives

The participants were generally positive about the relevance and value of the SRA. This is reflected in the responses to statement 1, 6, and 7.

R4 Highly granular – Method must facilitate granular description of assets and associated risks

The responses to statements 1 and 2 suggest that the granularity of the SRA is sufficient.

5.4. Evaluation conclusions

These outcomes are in line with the outcomes of the combined SWOT evaluation in Section 4.5 of the user workshops. The two main beliefs found there are also represented in the evaluation workshop outcomes. These are that firstly, the value of the SRA as an assessment and its output is recognised. The second belief is that it can be difficult to apply the SRA, as it requires time and varying expertise. Help during the application of the SRA is absolutely necessary, to guide the expertise of non-risk management experts.

6

Conclusion

6.1. Conclusions

This thesis set out to develop and test a method for assessing the societal risks of quantum computing, particularly in domains that use PKI systems. Using design science research, it was able to produce the SRA. Outcomes of the SRA provide users with answers as to why to invest in mitigating the quantum threat and where to begin. This SRA is, to the best of my knowledge, the first of its kind, combining risk assessment in information security with the consequences to society. This is important in a world ever increasingly dependent on digital communication.

The following statements summarise the application context of the SRA:

- The SRA can be applied by any party that is reliant on PKI and wants to know the risks they run in a societal context because of their PKI reliance.
- The SRA is designed to be domain unspecific and is expected to work similarly across domains.
- It is advised to perform the assessment with a team of experts with expertise in risk management, (senior) management, technology (i.e., PKI), potentially affected business processes, and compliance.
- It is advised that the assessment is guided by an assessment leader that is acquainted with the SRA method.
- The assessment is expected to take four to six hours.
- A report should be drawn up from the results of the assessment to maximise actionable insights.

It should be noted that although the SRA is expected to work similarly across domains, this has not been field tested. Further points on this are made in the reflections and recommendations. This also applies to the expected duration of the assessment and the best way to guide the assessment.

The results from the user workshops indicate a need for a method to properly assess the risks that the quantum threat brings. The SRA fulfils that need. Therefore, it answers the first research question: What are the components of a method to assess the potential societal effects of the quantum threat to PKI used by QTSPs? The eventual design holds up to the requirements of relevance and high granularity, but less so for the usable and transferable requirements. This is because applying the SRA properly

turned out to be a complex process that requires expertise in several areas: PKI, quantum computing, risk management, business processes, and compliance. Ways to improve these are discussed later in 6.3.

On the other hand, the diverse set of expertise areas is exactly what creates the most valuable insights in risk assessment. One-sided views do not help the assessing organisation in obtaining the value it could. Also, proper guidance during the assessment is crucial. It leads to a focused assessment which directly translates to better results. Another key aspect that drives the value of insights is the explanations accompanying the scores of the SRA. Without explanation, the scores mean very little and the SRA does not provide the answers it aims to.

After validating the case study of PKIgovernment and its Policy Authority, workshop participants indicated that assistance in applying the method is useful and necessary.

The second research question was: What are the potential societal effects of the quantum threat to PKIoverheid in the Netherlands? This was answered by performing a case study by applying the SRA from the perspective of Logius, the PA, with PKIoverheid as the object of analysis.

There are a myriad of ways in which society may be impacted if Logius is not able to secure PKIoverheid. Examples include interference with information exchange for medical professionals; leaking of company secrets of many companies operating in the Netherlands; potential loss of any application that uses DigiD facilitating communication between the Dutch government and citizens; large scale fraud because accountants, bailiffs, and notaries cannot securely sign documents; and leaking of military intelligence, as secure communications are very hard to set up.

Information security risks within an organisational context can impact society. This thesis has provided more insight into how these risks can be structurally assessed, by providing a method to do so. Additionally, the research serves as a stepping stone to assess the societal risks of the quantum threat to PKI. Something which is lacking in the literature. The designed SRA, findings in the user and evaluation workshops, and conclusions of this thesis contribute to the scientific progress of work package 1 of project HAPKIDO.

6.2. Reflections

A very important part of research is validity. By no means is this thesis unquestionable evidence of a foolproof method. It is however an indication that a method like this could work very well. Many experts, practitioners and researchers alike, gave their substantiated opinions about the SRA. This is important for the **content validity**, as it means the SRA is not likely to have any glaring gaps in what it aims to measure. However, the **construct validity** is less rigorous. In the user workshops and evaluation workshop, I only measured the participants' perceptions about the method. I have not measured for example the speed in which they were able to perform the SRA as part of the construct ease of use, or the amount of times a clarifying question was asked as part of the construct simplicity. But, this kind of construct validity rigour is also not seen in other risk assessment method research. As for **internal validity**, an important factor bringing it down is the fact that I myself performed the case study of Logius and PKIoverheid. The evaluation workshop participants then based their opinions on my implementation of the SRA and the results. The fact that they did not experience the process themselves may have influenced their opinions of the SRA. Lastly, the **external validity** of the SRA is relatively weak, as it was only tested once for the eGovernment domain and all feedback came from Dutch context. Furthermore, the participants in the evaluation workshop were all involved earlier in the design process, meaning the evaluation was not independent of the development. However,

although innovative, the SRA shares many building blocks with other RAs, which are proven in practise. Moreover, the practitioners in the user workshops were specifically selected based on their work in different sectors (eGovernment, banking, and telecom/trust service provision). These two facts speak for some external validity of the SRA.

Aside from the validity, there are some aspects of the SRA that need attention. One of these aspects is that the GRNV is intended to be used with specifically made threat scenarios. In the SRA, the threat scenarios that it is used for are found through granular risk identification as conventional in information security RA. This was sometimes not quite a smooth experience. Perhaps it would be better if a SecRAM-like scoring matrix based on the GRNV is developed to score the societal impact in step 3.2.2. Another aspect is the SecRAM scoring matrix for the organisational impact in step 3.1. As mentioned in Section 4.3.4, the scoring matrix can be adapted as deemed necessary by the assessor. However, it might be a good idea to have an example ready adapted to the specific case of PKI and the quantum threat, as this lowers the bar for assessors. The organisational impact scoring card as-is is good, but there might be room for improvement.

At around three quarters of the research timeline, it was discovered that business impact analyses could be a very useful input for the SRA. It even comes close to the SRA, as it aims to answer what would happen if certain business processes could not function anymore. However, it does not render the SRA unnecessary. While it does provide a less technical perspective, it is still limited to the organisational rather than societal (influence) scope. An issue with using business impact analyses in this research is that the information is confidential. Therefore, the SRA could not be specifically adapted to include a business impact analysis as input, but can only mention that it may be useful.

Other than the quantum threat to PKI, the SRA might be appropriate in general information security contexts in need of a societal perspective. After all, the world is ever more dependent on technological implementations and thus the societal dependencies are ever more important in other contexts as well. Perhaps with (or without) some adaptation, the SRA can provide a way to assess the societal risks of new technologies that present a threat, just as quantum computing does.

6.3. Recommendations

The recommendations of this thesis are targeted to three different audiences. First there are the intended users of the SRA. This is any party active in providing, maintaining, or making use of PKI-enabled trust services. I advise these parties to make use of this SRA, so as to shed light on the societal risks run by these parties rather than solely the organisational risks as is standard. This will show whether mitigation of the quantum threat is critical for the specific party and it will provide information on where to prioritise the efforts if necessary. Once done the first time, the SRA can be easily repeated, as only slight adaptations are likely. There may be business and technological changes that influence the insights provided. Expectations about the quantum threat and the mitigative capabilities will change over time. Both the development of a capable quantum computer and mitigative measures take time to implement, so reevaluation of the SRA over time is advisable. Doing the SRA can be included in the business continuity planning activities and may be done yearly until the quantum threat is completely mitigated. It is also advised after doing the SRA to look into mitigative measures outside of the scope of this research. CARAF can be applied to help the transition towards quantum safe cryptography.

Then there is the research community both outside and inside project HAPKIDO. I would advise researchers to develop the SRA further in three areas. Firstly, improve the transferability by making a manual departing from the SRA template in Appendix A, adding a exemplary case, and/or design-

ing a training workshop (video or face-to-face) for risk management experts. Secondly, to improve the usability, refine the impact estimation by investigating changing the organisational impact scoring matrix and changing the societal impact criteria and scoring procedure of the GRNV. Thirdly, it needs to be better understood how the SRA can be best applied. Group size and composition of the assessor and the option of a digital tool should be better explored. Another necessity is to take away the validation concerns raised in 6.2 above by rigorous research. An additional interesting avenue to pursue for researchers is to see whether the SRA is applicable to expected future technological changes that present a threat other than quantum computing. This point is also raised in 6.2.

As for the researchers in project HAPKIDO, aside from the points above, I advise you to do two things. First, make sure to evaluate the SRA by organising a larger evaluation session with more diverse partners from the project. Then let the SRA be applied to the banking and telecom/trust service provision domains in sessions with field experts and possibly do the same for eGovernment. After this, the SRA is ready to help answer the research question of WP1: What are the societal risks of a quantum-unsafe PKI in the quantum era? The SRA can be applied multiple times in cooperation with a representative selection of stakeholders. Then, the results can be combined to gain practical insight into the societal risks of the quantum threat to PKI in the Netherlands. Additionally, this research left PKIs not managed by QTSPs out of scope. For the purpose of WP1, it might be valuable to consider PKIs that are managed by the organisations that use them, such as the Ministry of Justice and Safety, the Ministry of Economic Affairs, and the Netherlands Vehicle Authority (RDW)[1]. Another important factor to consider is how trust loss in multiple domains can cause cascading or multiplicative impacts.

Concerning the other work packages of HAPKIDO, it should be noted that the SRA does not consider all types of risk relevant to HAPKIDO. The SRA is designed to assess the risks in case nothing is done to thwart the quantum threat. Essentially, it assesses the risks of failing PKI. However, there are two other types of risk very relevant to HAPKIDO. The first is mitigation risk. This is the risk resulting from taking mitigative measures, such as downscaling PKI usage and using other means to the same end. The second risk type is a form of mitigation risk: migration risk. This is the risk that arise from migrating to a quantum safe PKI. These include not knowing where all leaf certificates are, implementation mistakes, and hardware restrictions at the end-user level. These types of risk should be considered in the rest of project HAPKIDO.

Lastly, I would like to advise policy makers on the national and inter-organisational level to look into the quantum threat and its societal risks. On the national and inter-organisational level, policy makers have the power to influence actors on the organisational level, which is where the eventual change to quantum safe cryptography needs to take place. Policy makers should keep a close eye on project HAPKIDO. Although the project is not yet finished, it will provide lessons for transitioning to quantum safe PKI in the near future. For now, use of the SRA can be incentivised to create a sense of urgency and help prepare for the transition.

[1] https://kennisopenbaarbestuur.nl/media/256209/onderzoek_stimulering-pkioverheid-innovalor_19-4-2019.pdf, p. 12 & 14

References

Algemene Inlichtingen- en Veiligheidsdienst. (2021, September). *Bereid je voor op de dreiging van quantum computers*. https://www.aivd.nl/binaries/aivd_nl/documenten/publicaties/2021/09/23/bereid-je-voor-op-de-dreiging-van-quantumcomputers/Brochure+Dreiging+Quantumcomputers%5C%2C+webversie+september+2021.pdf

Amadori, A., Duarte, J. D., & Spini, G. (2022, March 31). Literature overview of public-key infrastructures, with focus on quantum-safe variants deliverable 4.1, HAPKIDO project.

Analistennetwerk Nationale Veiligheid. (2019, May). *Leidraad risicobeoordeling geïntegreerde risicoanalyse nationale veiligheid*. https://www.rivm.nl/sites/default/files/2019-10/Leidraad%5C%20Risicobeoordeling%5C%202019.pdf

Aven, T. (2018). An emerging new risk analysis science: Foundations and implications. *Risk Analysis*, *38*(5), 876–888. https://doi.org/10.1111/risa.12899

Aven, T., Andersen, H. B., Cox, T., Droguett, E. L., Greenberg, M., Guikema, S., Kröger, W., McComas, K., Renn, O., Thompson, K. M., & Zio, E. (2018, August). *Core subjects of risk analysis*. Society for Risk Analysis. https://www.sra.org/wp-content/uploads/2020/04/SRA-Core-Subjects-R2.pdf

Bharosa, N., Wijk, R. v., Winne, N. d., & Janssen, M. (2015). *Challenging the chain: Governing the automated exchange and processing of business information*. IOS Press Ebooks. https://doi.org/10.3233/978-1-61499-497-8-i

Bruijn, H. d., & Heuvelhof, E. T. (2008). Strategies: A comparison between project-based and process-based change. *Management in networks*. Routledge.

Davenport, T. H., & Short, J. E. (1990). The new industrial engineering: Information technology and business process redesign. *Sloan Management Review*, *31*(4), 11–27. Retrieved April 14, 2022, from https://sloanreview.mit.edu/article/the-new-industrial-engineering-information-technology-and-business-process-redesign/

de Wolf, R. (2017). The potential impact of quantum computers on society. *Ethics and Information Technology*, *19*(4), 271–276. https://doi.org/10.1007/s10676-017-9439-z

Esteves, A. M., Franks, D., & Vanclay, F. (2012). Social impact assessment: The state of the art. *Impact Assessment and Project Appraisal*, *30*(1), 34–42. https://doi.org/https://doi.org/10.1080/14615517.2012.660356

Gill, S., Kumar, A., Singh, H., Singh, M., Kaur, K., Usman, M., & Buyya, R. (2021). Quantum computing: A taxonomy, systematic review and future directions. *Software - Practice and Experience*. https://doi.org/10.1002/spe.3039

Gregor, S. (2006). The nature of theory in information systems. *MIS Quarterly*, *30*(3), 611–642. https://doi.org/10.2307/25148742

Hevner, A. R. (2007). A three cycle view of design science research. *Scandinavian Journal of Information Systems*, *19*(2). https://aisel.aisnet.org/sjis/vol19/iss2/4

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, *28*(1), 75–105. https://doi.org/10.2307/25148625

International Organization for Standardization [ISO]. (2018). *Information technology — security techniques — information security management systems — overview and vocabulary* (ISO/IEC 27000:2018). Retrieved April 14, 2022, from https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en

Joosten, R., & Smulders, A. (2014). *How to successfully manage risks in hyperconnected value networks*. TNO. http://resolver.tudelft.nl/uuid:95b1a97a-2d5c-41b1-b5d9-43bcd04d981b

Joseph, D., Misoczki, R., Manzano, M., Tricot, J., Pinuaga, F. D., Lacombe, O., Leichenauer, S., Hidary, J., Venables, P., & Hansen, R. (2022). Transitioning organizations to post-quantum cryptography. *Nature*, *605*(7909), 237–243. https://doi.org/10.1038/s41586-022-04623-2

Le Fevre, M., Gölz, B., Flohr, R., Stelkens-Kobsch, T., & Verhoogt, T. (2017). *SecRAM 2.0: Security risk assessment methodology for SESAR 2020*. SESAR. https://www.sesarju.eu/sites/default/files/documents/transversal/SESAR%5C%202020%5C%20-%5C%20Security%5C%20Reference%5C%20Material%5C%20Guidance.pdf

Lindsay, J. R. (2020). Demystifying the quantum threat: Infrastructure, institutions, and intelligence advantage. *Security Studies*, *29*(2), 335–361. https://doi.org/https://doi.org/10.1080/09636412.2020.1722853

Logius. (2022, March 1). Programme of requirements part 1: Introduction [Ver. 4.10]. Retrieved June 1, 2022, from https://www.logius.nl/sites/default/files/public/bestanden/diensten/PKIoverheid/PoR-2022/PKIoverheid%5C%20Programme%5C%20of%5C%20Requirements%5C%20v4.10%5C%20-%5C%20Part%5C%201%5C%20Introduction.pdf

Ma, C., Colon, L., Dera, J., Rashidi, B., & Garg, V. (2021). CARAF: Crypto agility risk assessment framework. *Journal of Cybersecurity*, *7*(1), 1–11. https://doi.org/10.1093/cybsec/tyab013

Mavroeidis, V., Vishi, K., Zych, M. D., & Jøsang, A. (2018). The impact of quantum computing on present cryptography. *International Journal of Advanced Computer Science and Applications (ijacsa)*, *9*(3). https://doi.org/10.14569/IJACSA.2018.090354

Mosca, M., & Mulholland, J. (2017, January 5). *A methodology for quantum risk assessment* (Whitepaper). Global Risk Institute. https://globalriskinstitute.org/download/a-methodology-for-quantum-risk-assessment-pdf/

Mosca, M., & Piani, D. M. (2021, January). *Quantum threat timeline report 2020*. Global Risk Institute. https://globalriskinstitute.org/publications/quantum-threat-timeline-report-2020/

Mulholland, J., Mosca, M., & Braun, J. (2017). The day the cryptography dies. *IEEE Security Privacy*, *15*(4), 14–21. https://doi.org/10.1109/MSP.2017.3151325

Presley, A., & Liles, D. (1998). The use of IDEF0 for the design and specification of methodologies. https://www.researchgate.net/publication/2447898_The_Use_of_IDEF0_for_the_Design_and_Specification_of_Methodologies

Raban, Y., & Hauptman, A. (2018). Foresight of cyber security threat drivers and affecting technologies. *Foresight*, *20*(4), 353–363. https://doi.org/10.1108/FS-02-2018-0020

Shamala, P., Ahmad, R., & Yusoff, M. (2013). A conceptual framework of info structure for information security risk assessment (ISRA). *Journal of Information Security and Applications*, *18*(1), 45–52. https://doi.org/10.1016/j.jisa.2013.07.002

Skosana, U., & Tame, M. (2021). Demonstration of shor's factoring algorithm for n = 21 on IBM quantum processors. *Scientific Reports*, *11*(1), 16599. https://doi.org/10.1038/s41598-021-95973-w

Smart, N. P. (2016). *Cryptography made simple*. Springer Cham. https://doi.org/10.1007/978-3-319-21936-3

Spini, G. (2020, September 14). Hybrid approach for quantum-safe public key infrastructure development for organisations (HAPKIDO).

Stake, R. (2003). Case studies. In N. K. Denzin & Y. S. Lincoln (Eds.), *Strategies of qualitative inquiry* (2nd ed). Sage.

TNO. (n.d.). *Analistennetwerk Nationale Veiligheid (ANV)* [TNO]. Retrieved March 16, 2022, from https://www.tno.nl/nl/aandachtsgebieden/defensie-veiligheid/roadmaps/nationale-veiligheid/crisisbeheersing-nieuwe-uitdagingen-nieuwe-kansen/analistennetwerk-nationale-veiligheid/

Vermaas, P. E. (2017). The societal impact of the emerging quantum technologies: A renewed urgency to make quantum theory understandable. *Ethics and Information Technology*, *19*(4). https://doi.org/10.1007/s10676-017-9429-1

Wadhwa, K., Barnard-Wills, D., & Wright, D. (2015). The state of the art in societal impact assessment for security research. *Science and Public Policy*, *42*(3), 339–354. https://doi.org/10.1093/scipol/scu046

Wangen, G., Hallstensen, C., & Snekkenes, E. (2018). A framework for estimating information security risk assessment method completeness. *International Journal of Information Security*, *17*(6), 681–699. https://doi.org/10.1007/s10207-017-0382-0

Yunakovsky, S. E., Kot, M., Pozhar, N., Nabokov, D., Kudinov, M., Guglya, A., Kiktenko, E. O., Kolycheva, E., Borisov, A., & Fedorov, A. K. (2021). Towards security recommendations for public-key infrastructures for production environments in the post-quantum era. *EPJ Quantum Technology*, *8*(1), 1–19. https://doi.org/10.1140/epjqt/s40507-021-00104-z

A

SRA template

Step 0: Determine the scope of the assessment

The Societal Risk Assessment (SRA) makes use of three scopes. The technological scope determines what technologies are considered and which are left out of the assessment. The organisational scope determines which part(s) of which organisation(s) are considered as the party that bears the consequences of the identified risks. Lastly, the societal influence scope delineates the reach of the risks within society, outside of the organisational scope. It is important to set these scopes beforehand, so that all participants' thinking is aligned.

Table A.1: Step 0 template

Method/framework	Scope
Technological	The technological scope is limited to • risks that emerge from quantum computing • risks related to PKI • …
Organisational	…
Societal influence	…
Explanation:	

Step 1: Examine the threat to guard against

The threats are that which to defend against. Threats are enabled by exploiting a vulnerability. Both threats and vulnerabilities are informed by the technological scope from Step 0. By knowing what to defend against and what enables that, we can later identify what is vulnerable to attack.

Table A.2: Step 1 template

Threat	**Vulnerability**
Quantum computing breaking asymmetric cryptography real-time 'Store now, decrypt later' tactic capturing sensitive data in-transit protected by PKI …	The use of any cryptographic solution dependent on the discrete log or factorisation problems (e.g., RSA, ECC, DH), which can be broken by quantum computing (i.e., virtually all asymmetric cryptography in place) …

Explanation: ⋯

Step 2: Make an inventory of assets

The assets are that which to protect. This can be anything of value to the assessing organisation. The results from Step 1 are used to select only assets relevant to the assessment. The SRA defines three kinds of assets: business processes, (PKI) applications, and services.

Business process:	A wide range of structured, often chained, activities or tasks conducted by people or equipment to produce a specific service or product for a particular user or consumer.
Application:	A use to which the examined technology, PKI, is put.
Service:	The execution of information processes provided by an organisation.

Every asset is informed by the technological scope. Business processes fall within the organisational scope. Applications can be part of the organisational scope or the societal influence scope, depending on the organisational structure. Services are part of the societal influence scope, as these are services provided to society.

Table A.3: Step 2 template

Business process Organisational	**Application** Org. / Soc. influence	**Service** Societal influence
		…
	…	…
		…
		…
…	…	…
		…
		…
	…	…
		…

Explanation: …

Step 3: Estimate impacts

Step 3.1: Estimate organisational impacts

The impacts of the threats from Step 1 on the assets of Step 2 are now assessed. First, the organisational impacts are assessed, meaning the impacts limited to the organisational scope. These are assessed for situations in which information security properties cannot be guaranteed for a business process. The information security properties are confidentiality, integrity, and availability.

Confidentiality: property that information is not made available or disclosed to unauthorised individuals, entities, or processes.

Integrity: property of accuracy and completeness.

Availability: property of being accessible and usable on demand by an authorised entity.

To find the correct organisational impact scores, the table on page 8 is used. After filling in the scores, copy the highest score to the 'Total' column.

Table A.4: Step 3.1 template

Business process	**CIA**	**Personnel**	**Capacity**	**Performance**	**Economic**	**Branding**	**Regulatory**	**Environment**	**Total**
	C	…	…	…	…	…	…	…	…
…	I	…	…	…	…	…	…	…	…
	A	…	…	…	…	…	…	…	…
	C	…	…	…	…	…	…	…	…
…	I	…	…	…	…	…	…	…	…
	A	…	…	…	…	…	…	…	…

Explanation: …

Table A.5: Organisational impact score card taken from SecRAM (Le Fevre et al., 2017)

Impact Areas	A No impact	B Minor	C Severe	D Critical	E Catastrophic
Personnel	No injuries	Minor injuries	Severe injuries	Multiple severe injuries	Fatalities
Capacity	No capacity loss	Loss of up to 10% capacity	Loss of 10% - 30% capacity	Loss of 30% - 60% capacity	Loss of 60% - 100% capacity
Performance	No quality abuse	Minor system quality abuse	Severe quality abuse that makes systems partially inoperable	Major quality abuse that makes major system inoperable	Major quality abuse that makes multiple major systems inoperable
Economic	No effect	Minor loss of income	Large loss of income	Serious loss of income	Bankruptcy or loss of all income
Branding	No impact	Minor complaints	Complaints and local attention	National attention	Government & international attention
Regulatory	No impact	Minor regulatory infraction	Multiple minor regulatory infractions	Major regulatory infraction	Multiple major regulatory infractions
Environment	Insignificant	Short term impact on environment	Severe pollution with noticeable impact on environment	Severe pollution with long term impact on environment	Widespread or catastrophic impact on environment

Step 3.2: Estimate societal impacts

This part of the assessment is done with a view that stretches further than the organisational scope. Here, the societal influence scope is applied. To get to the societal impacts, first the end-user impacts are assessed.

Step 3.2.1: Estimate end-user impact

Assess what the impact on end-users is if an information security property cannot be guaranteed anymore. This impact takes the form of a short-written answer in which the consequences for end-users are described.

Table A.6: Step 3.2.1 template

Business process	⋯	
Application	**CIA**	**Consequences for end-users**
	C	⋯
⋯	I	⋯
	A	⋯
	C	⋯
⋯	I	⋯
	A	⋯

Explanation: ⋯

Step 3.2.2: Estimate impacts on national security

For each business process, fill in the table assessing the impact on national security a compromise of the applications related to the business process has. The scoring is done using the Leidraad risicobeoordeling Geïntegreerde risicoanalyse Nationale Veiligheid (GRNV). Use the results from Step 3.2.1 to help the scoring. After filling in the scores, copy the highest score to the 'Total' column.

Table A.7: Step 3.2.2 template

Business process	**CIA**	**International position 1.2**	**Cyberspace 1.3**	**Costs 3.1**	**Economy 3.2**	**Day-to-day life 5.1**	**Rule of law 5.2**	**…**	**Total**
	C	…	…	…	…	…	…	…	…
…	I	…	…	…	…	…	…	…	…
	A	…	…	…	…	…	…	…	…
	C	…	…	…	…	…	…	…	…
…	I	…	…	…	…	…	…	…	…
	A	…	…	…	…	…	…	…	…

Explanation: …

Step 4: Estimate likelihood

Because it is uncertain when a large enough quantum computer will be available, in this step the time to act is approximated. To do so, the following variables are estimated for each business process.

X =	longest shelf life of data within the scope of the business process [years]
Y =	time it will take to replace all vulnerable cryptography used within the scope of the business process to quantum safe cryptography [years]
Z =	estimated time until a powerful enough quantum computer is available [years] (may vary depending on risk appetite)
t =	theoretical time to act [years]

The resulting theoretical time to act (t) is not an exact figure and should not be interpreted as such. It is based on three estimates and is therefore an approximation.

Table A.8: Step 4 template

Business process	X	Y	Z	**Threat**	**Formula for t**	t
…	…	…	…	Real-time access (CIA)	t = Z – Y	⋯
				Store now, decrypt later (C)	t = Z – X – Y	⋯
…	…	…	…	Real-time access (CIA)	t = Z – Y	⋯
				Store now, decrypt later (C)	t = Z – X – Y	⋯
…	…	…	…	Real-time access (CIA)	t = Z – Y	⋯
				Store now, decrypt later (C)	t = Z - X – Y	⋯
…	…	…	…	Real-time access (CIA)	t = Z – Y	⋯
				Store now, decrypt later (C)	t = Z – X – Y	⋯

Explanation: ⋯

Step 5: Combine results

The results from all previous steps are combined in a single table. The organisational and national impact are taken from Steps 3.1 and 3.2.2 respectively. The theoretical time to act (t) is taken from Step 4. Lastly, using the conversion matrix, the risks can be ranked. Taking the highest of the two impact scores and the theoretical time to act, the matrix ranks the risk for each threat to each business process. It should be noted that the conversion matrix can be adjusted according to the risk appetite of the assessing organisation.

Table A.9: Step 5 overview template

Business process	**Threat**	**Organisational impact**	**National impact**	t
…	Real-time access (CIA)	…	…	…
	Store now, decrypt later (C)	…	…	…
…	Real-time access (CIA)	…	…	…
	Store now, decrypt later (C)	…	…	…
…	Real-time access (CIA)	…	…	…
	Store now, decrypt later (C)	…	…	…
…	Real-time access (CIA)	…	…	…
	Store now, decrypt later (C)	…	…	…

Explanation: …

Table A.10: Step 5 conversion matrix example

Impact score	t			
	> 5	$4 - 0$	$-1 - -5$	< -5
A	Acceptable	Acceptable	Moderate	Moderate
B	Acceptable	Acceptable	Moderate	Severe
C	Acceptable	Moderate	Severe	Severe
D	Moderate	Severe	Severe	Critical
E	Severe	Severe	Critical	Critical

Table A.11: Step 5 synthesis results template

Business process	Threat	Risk category
…	Real-time access (CIA)	⋯
	Store now, decrypt later (C)	⋯
…	Real-time access (CIA)	⋯
	Store now, decrypt later (C)	⋯
…	Real-time access (CIA)	⋯
	Store now, decrypt later (C)	⋯
…	Real-time access (CIA)	⋯
	Store now, decrypt later (C)	⋯

Explanation: ⋯

B

User workshop outcomes

In this appendix, all workshops outcomes are documented. First the user workshops and second the output evaluation workshop. For every workshop, the following details are specified: date, SRA version used for the workshop, and the participants present. Additionally, a SWOT analysis of the SRA version is presented related to the workshop. For the user workshops, the SWOT analysis was performed by myself, based on the comments and feedback received in and overall progress of the workshop. Then, after every SWOT analysis, the choices for the next SRA version are laid out in a table. As for the output evaluation workshop, the SWOT analysis was a collaborative effort during the workshop as a final evaluation. Therefore, no choices were made for a new SRA version. The combined SWOT analysis in Chapter 4 was made by bundling similar notions of strengths, weaknesses, opportunities, and threats of all SWOTs together and leaving out those that were dealt with in newer versions of the SRA.

User workshop 1

Table B.1: User workshop 1 details

Date	02-11-2021
SRA version	0.1
Participants	PKI manager at PA, manager at TSP, cyber security of critical infrastructures scientist

Table B.2: User workshop 1 SWOT analysis of the SRA

Strengths • Threat capacities are clear and recognised • Necessity is recognised • The trust supply side sees the potential of the method	**Weaknesses** • Does not include cyber criminals as a threat actor [c] • Does not recognise that anyone may eventually acquire access to quantum computing [o]
Opportunities • Make use of existing Business Impact Analyses [r] • Invest in storytelling [a] • Present the three impact levels visually	**Threats** • Skipping national impact areas may leave some impacts unidentified [b]

Table B.3: User workshop 1 SRA design choices

v0.1 → v0.2	
Choice	**Rationale**
[a] Add a text box beneath each table to be filled in, that is used to add context to the choices made in the tables. Applies to all steps.	The audience from workshop 1 gave the feedback that storytelling is important to convey the message and reach the goals of this SRA. Moreover, it allows for elaboration on the choices made during the application process of the SRA.
[b] Include all national impact criteria from the GRNV instead of a selection	The audience of workshop 1 indicated that there were relevant impacts outside of the initially selected impact areas. There is a risk of not capturing all relevant impacts when leaving out impact areas.
[c] Add cybercriminals to the threat actors	Cybercriminals are potential threat actors as well. These were initially overlooked.

User workshop 2

Table B.4: User workshop 2 details

Date	13-12-2021
SRA version	0.2
Participants	M2M communication program lead at a large bank

Table B.5: User workshop 2 SWOT analysis of the SRA

Strengths • There are many different applications/-solutions dependent on PKI which are captured by the asset identification step (e.g. all customer interfaces; My business, my data; BIV; SSC) • Organisational impact matrix is intuitive and invites discussion • Very recognisable method • Different levels of analysis make sense	**Weaknesses** • It does not matter so much what threat actor attacks for the societal effects [o] • The terms friendly and hostile state actor are not nuanced enough to reflect reality [d o]
Opportunities • Couple likelihood of scenarios with the threat actors [o] • Add a middle layer state actor category [d]	**Threats** • The likelihood is very hard to properly identify

Table B.6: User workshop 2 SRA design choices

v0.2 → v0.3	
Choice	**Rationale**
[d] Refrain from adding extra middle layer state actor category	This is not likely to increase the quality of the output. It will not capture the nuance as it is still too limited and will also weaken the focus of the analysis.

Table B.7: User workshop 2 additional insights

Additional relevant insights
The bank has firmly committed to digitalisation and the use of certificates. The entire modern way of banking is reliant on certificates. In the worst case we will have to fall back to a 'paper society'.
The large bank is planning to employ a QTSP to provide QES technology for its digital trust needs.
For various processes that the bank fulfils, several different types of certificates are used that rely on differing PKI structures.
When all Dutch electronic financial transaction traffic is interrupted for half a day, all of the Netherlands will be bankrupt.
There is no other sector that has more societal impact than the financial sector when it is interrupted, even healthcare.

User workshop 3

Table B.8: User workshop 3 details

Date	12-01-2022
SRA version	0.3
Participants	PKI manager at QTSP, compliance officer at QTSP, technical expert at QTSP

Table B.9: User workshop 3 SWOT analysis of the SRA

Strengths • Making an inventory of PKI applications and peeling off each layer of impact is a good approach • The inclusion of multiple perspectives	**Weaknesses** • No distinction between compromise and mitigation risks [h]
Opportunities • Have the outcome of the RA be a prioritisation of assets to make quantum safe first [g] • Leave room for a broad perspective of risk and cascading effects of trust loss [t] • Mind the PKI use-case as it affects the impacts [e] • Include the risks that come with transitioning to QS PKI [f] • Use the term 'applications' to indicate assets that make use of PKI [e]	**Threats** • The term 'assets' can be interpreted too broadly [e] • The absence of a distinction between compromise and mitigation risks can muddy the discussion [h]

Table B.10: User workshop 3 SRA design choices

v0.3 → v0.4		
	Choice	**Rationale**
e	Change the term 'asset' to 'application'	'Application' better reflects the use of PKI rather than the technical components behind it
f	Explicitly keep the risks of transitioning/migrating to QS PKI out of scope	This best reflects the original research question of HAPKIDO WP1 upon which this research is based
g	Have the last step be a prioritisation of risks	Not all systems can be simultaneously updates to be QS, therefore it is important to identify the biggest risks so they can be mitigated first
h	Scope the RA to risks of compromise and keep mitigation measures and their risks out of scope	It is better fitting for this research and HAPKIDO WP1 to focus on the risks that emerge from not acting. Additionally, the different types of compromise cover potential mitigation risks for a large part.
t	Have the national impact judged per business process	By combining the trust loss of all affected applications, the assessor is free to speculate about a scenario used for the national impact assessment including cascading loss of trust

Table B.11: User workshop 3 additional insights

Additional relevant insights
The level of trust demanded by the market is expected to keep increasing. As the demand for a higher level of trust increases, so does the demand for qualified trust services, as qualification is a means to ensure a high level of trust.
Some assets are less sensitive/critical than others and it is not realistic to make all systems quantum safe at once.

User workshop 4

Table B.12: User workshop 4 details

Date	26-01-2022
SRA version	0.4
Participants	M2M communication program lead at tax authority, risk management expert

Table B.13: User workshop 4 SWOT analysis of the SRA

Strengths • Organisational impact assessment feels familiar, invites discussion, and is workable • Individual impact assessment is workable	**Weaknesses** • Friendly state actors are not really a clear concept, as they can still employ hostile activities [o] • The term 'applications' is ambiguous as it can mean a technical component using PKI as well as a business process in which PKI is applied [k] • Lack of specific scoping can muddy the discussion and decrease the quality of the outcomes [l m n]
Opportunities • Define state actors by their motivation to spy or disrupt [o] • The assessor can decide the level of analysis when deciding on the assets: applications can be subdivided in domains per application in order to group the dependent services [i] • Similarly, applications can be grouped into application groups [i]	**Threats** • The list of dependent services per application can get quite long [i] • Organisational impact: capacity & performance may be differently interpreted by different assessing parties, depending on their industry [s]

Table B.14: User workshop 4 SRA design choices

v0.4 → v0.5		
	Choice	**Rationale**
i	Make explicit that it is the duty of the assessor to decide the proper level of analysis for the assets	Different situations call for different levels of analysis. The assessor is able to see the specific situation and can choose the appropriate level of analysis, rather than the method specifying a specific level of analysis for all situations.
j	Abstain from explicitly incorporating levels of confidentiality	Difference in levels of confidentiality is reflected in impacts. The impact of highly confidential information leaking will be higher. In the end, the impact resulting from the level of confidentiality is what counts. Additionally, it is reflected in the time to act when considering a store now, decrypt later attack.
k	Separate applications and business processes when making an inventory of assets	The two concepts need to be separated as it can cause confusion to only use 'applications'. This allows for the assessor to link the two together and get a clear picture of what is discussed.
l	Add an extra step beforehand for specifying the scopes used in the RA	Lack of specific scoping can hinder the analysis and decrease the quality of output
m	Introduce three different scopes: technical, organisational, and societal influence	These three scopes should keep the discussions focussed. The technical scope limits the discussion to the relevant technologies
n	Put the organisational impact assessment before the identification of services to society	By swapping these steps, the assessor stays within the organisational scope before taking a broader societal perspective. The aim is to reduce confusion because of scope switching.
o	Change the threat assessment to identifying threats and vulnerabilities that can be exploited by the threats, leaving out threat actors	For this type of risk assessment, the threat actor does not really matter. In the end, the attacks and following impacts are all the same.
s	Abstain from further defining the impact areas capacity & performance in the organisational impact	The room for interpretation in these impact areas is a necessary evil. This way, the SRA is more widely applicable as different parties in the trust chain may have different kinds of capacity.

Table B.15: User workshop 4 additional insights

Additional relevant insights
By using PKI, the tax authority gathers and sends data from and to many kinds of actors for various business processes.
Realising that there is a threat might be the biggest obstacle in transitioning to a QS version of SBR.
Going back to paper is not a viable option.
Right now, within the organisation there is not enough thought on how risks will play out nationally in a broad context. It is necessary to place risks in a broad perspective.

User workshop 5

Table B.16: User workshop 5 details

Date	24-02-2022
SRA version	0.5
Participants	PKI manager at PA, cyber security scientist

Table B.17: User workshop 5 SWOT analysis of the SRA

Strengths • The goal this method sets out to achieve is very relevant	**Weaknesses** • Switching between making an inventory of assets and assessing the impacts was confusing [p] • Terms are not clearly defined [q]
Opportunities • Documents such as a Business Impact Analyses and previously done risk assessments can be valuable input [r]	**Threats** • Parties are not likely to share sensitive information about their perceived vulnerabilities such as a Business Impact Analysis and previously done risk assessments [r]

Table B.18: User workshop 5 SRA design choices

v0.5 → v1.0		
	Choice	**Rationale**
[p]	Swap back the steps making an inventory of dependent services and organisational impact assessment	Switching between making an inventory of assets and assessing the impacts turned out to be confusing. Keeping them separate and switching between the organisational and societal influence scope seems better.
[q]	Give a clear definition for all terms used in the template	Clear definitions avoid confusion and improve the quality and speed of the analysis
[r]	Make explicit what input documents might be of use	Increased quality of input means increased quality of output. As most serious organisations should have useful input documents available, it is wise to make use of them.

Table B.19: User workshop 5 additional insights

Additional relevant insights
Any method that helps taking steps in dealing with the quantum threat to PKI is welcome.
The method can be used making use of confidential input documents but can also be used without these documents to arrive at more general output.
Most serious organisations should have a Business Continuity Plan, including a Business Impact Analysis and risk assessments.

Output evaluation workshop

Table B.20: Output evaluation workshop details

Date	12-01-2022
SRA version	1.0
Participants	PKI manager at PA, government and technology researcher, two cybersecurity researchers familiar with risk assessment

Table B.21: Output evaluation workshop SWOT analysis of the SRA

Strengths • Step-wise approach • Per business domain insights in the risks, dependencies, and potential impacts • One of a kind combining PKI and quantum computing	**Weaknesses** • Requires a lot of knowledge on business processes • Risk assessment process is hard for many business owners, because some information is hard to quantify • Difficult to pull mitigation strategies out of (although that was not necessarily the goal) • Required level of detail of information is hard to find
Opportunities • Insight into risks, making the quantum threat tangible • Insight in dependencies • Do a self assessment based on the SRA and combine it with recommendations/action pathways	**Threats** • Method can become to lengthy and complex, unclear why we need all these insights • Complexity of applying the method

C

Case study outcome

Step 0: Determine the scope of the assessment

The Societal Risk Assessment (SRA) makes use of three scopes. The technological scope determines what technologies are considered and which are left out of the assessment. The organisational scope determines which part(s) of which organisation(s) are considered as the party that bears the consequences of the identified risks. Lastly, the societal influence scope delineates the reach of the risks within society, outside of the organisational scope. It is important to set these scopes beforehand, so that all participants' thinking is aligned.

Table C.1: Step 0

Method/framework	Scope
Technological	The technological scope is limited to • risks that emerge from quantum computing • risks related to PKI • data at-rest, in-use, and in-transit • data protected by asymmetric cryptography
Organisational	The organisational scope relates to Logius, specifically Stelsels en Standaarden, the department responsible for maintaining and developing PKIoverheid (PKIo)[1].
Societal influence	The societal influence scope consists of the influence the organisation has on the members of Dutch society, other organisations, their interactions, and the functioning of Dutch society as a whole.

Explanation: The technological scope is formulated such that the quantum threat to PKI is the focus. All data with protection dependent on asymmetric cryptography is within scope, as that is way more vulnerable to QC than symmetric cryptography.

The organisational and societal influence scope are formulated so that PKIo and its influence on Dutch society are the focal points.

Step 1: Examine the threat to guard against

The threats are that which to defend against. Threats are enabled by exploiting a vulnerability. Both threats and vulnerabilities are informed by the technological scope from Step 0. By knowing what to defend against and what enables that, we can later identify what is vulnerable to attack.

Table C.2: Step 1

Threat	Vulnerability
Quantum computing breaking asymmetric cryptography real-time 'Store now, decrypt later' tactic capturing sensitive data in-transit protected by PKI	The use of any cryptographic solution dependent on the discrete log or factorisation problems (e.g., RSA, ECC, DH), which can be broken by quantum computing (i.e., virtually all asymmetric cryptography in place)

Explanation: The quantum threat to PKIo can be separated in two attack scenarios or threats. Both exploit the same vulnerability opened by quantum computing. The 'store now, decrypt later' tactic can be deployed right now and will be successful once the decryption can be broken and the data shelf life has not passed yet. The drawback is the power of the attack, as only the confidentiality of the data will be compromised.

Breaking asymmetric cryptography real-time is a much more powerful attack, as next to the confidentiality, the integrity and availability of the data can be compromised as well. This enables much more sophisticated and far-reaching attacks. However, this can only be done once quantum computing is developed enough.

Both these attacks compromise the trust created by PKIo and threaten Logius' goals and PKIo-facilitated services to society.

Step 2: Make an inventory of assets

The assets are that which to protect. This can be anything of value to the assessing organisation. The results from Step 1 are used to select only assets relevant to the assessment. The SRA defines three kinds of assets: business processes, (PKI) applications, and services.

Business process:	A wide range of structured, often chained, activities or tasks conducted by people or equipment to produce a specific service or product for a particular user or consumer.
Application:	A use to which the examined technology, PKI, is put.
Service:	The execution of information processes provided by an organisation.

Every asset is informed by the technological scope. Business processes fall within the organisational scope. Applications can be part of the organisational scope or the societal influence scope, depending on the organisational structure. Services are part of the societal influence scope, as these are services provided to society.

Table C.3: Step 2

Business process Organisational	**Application** Org. / Soc. influence	**Service** Societal influence
Trustworthiness assurance of the Organisation Person Domain	Defensiepas[2]	Authentication for ordering military materials, accessing buildings and remote systems on mission/from home, signing police reports for immigrant processing[3]
	Personal UZI-pas[4]	Sharing medical information between medical professionals, signing digital documents
	Taxi driver & inspector certificates[5]	Logging working hours and negating fraud
	eHerkenning 4	?
	Profession certificates[6]	Signing legally binding documents for accountants, bailiffs, notaries

Continued on next page

[2] https://magazines.defensie.nl/materieelgezien/2021/03/07_defensiepas
[3] Personal contact with Logius employee
[4] https://www.uziregister.nl/uzi-pas/waarvoor-heeft-u-een-uzi-pas-nodig
[5] https://bct.tsp.minienw.nl/minienw-bct-cps-g3/minienw-bct-cps-G3.pdf, p. 11
[6] https://certificaat.kpn.com/pkioverheidcertificaten/beroepscertificaten/

Table C.3 – *Continued from previous page*

Business process Organisational	**Application** Org. / Soc. influence	**Service** Societal influence
Trustworthiness assurance of the Organisation Services Domain	DigiD (organisation)[7]	Digital communication between civilians and governments
	UZI-servercertificate[8]	Sharing medical information between medical professionals
	eHerkenning	Digital communication between businesses and governments
	eSeals[9]	Proving integrity and non-repudiation on documents from organisations for e.g. EPREL
	Taxi business & inspection certificates[10]	Logging working hours and negating fraud
Trustworthiness assurance of the Citizen Domain	Vidua[11]	Signing of legal documents such as housing, job, or business contracts
	DigiD Substantieel & Hoog (citizen)[12]	Extra sensitive communication between citizens and governments (e.g., medical)
Trustworthiness assurance of the Autonomous Devices Domain	Taxi On-board Computer[13]	Logging working hours and negating fraud
Trustworthiness assurance of the public root CA	Inherited by four domains above	Inherited by four domains above
Trustworthiness assurance of the Private Services Domain	Digipoort[14]	Tax reports and other financial messages from businesses to several governments

Continued on next page

[7] https://www.logius.nl/diensten/digid/documentatie/functionele-beschrijving-digid
[8] https://www.uziregister.nl/uzi-pas/waarvoor-heeft-u-een-uzi-pas-nodig
[9] https://certificaat.kpn.com/pkioverheidcertificaten/services-certificaten/eseal/
[10] https://bct.tsp.minienw.nl/minienw-bct-cps-g3/minienw-bct-cps-G3.pdf, p. 11
[11] https://cleverbase.com/en/vidua-services/
[12] https://www.logius.nl/diensten/digid/documentatie/functionele-beschrijving-digid
[13] https://bct.tsp.minienw.nl/minienw-bct-cps-g3/minienw-bct-cps-G3.pdf, p. 11
[14] https://certificaat.kpn.com/pkioverheidcertificaten/servercertificaten/digipoort-private/

Table C.3 – *Continued from previous page*

Business process Organisational	**Application** Org. / Soc. influence	**Service** Societal influence
	Digikoppeling[15]	Automatic processing of data requests within the Dutch government
	ESDN[16]	B2B M2M communications in the energy sector
Trustworthiness assurance of the Private Person domain	Not currently in use[17]	Not currently in use
Trustworthiness assurance of the private root CA	Inherited by two domains above	Inherited by two domains above

Explanation: Logius is the Policy Authority (PA) of PKIo. It is therefore responsible for the trustworthiness of the entire PKIo[18]. To achieve this, three main tasks are named in the Certificate Practise Statement (CPS) and Programme of Requirements (PoR): Maintaining the PoR, overseeing admission of new Trust Service Providers (TSPs), and regulating and monitoring TSP activities under the PKIo root. These tasks could be regarded as the business processes in the assessment. However, they are not directly threatened by the threats identified in Step 1. Additionally, they provide no grounds for the separation of applications and services, as each task serves every application and service supported by PKIo. Therefore, the choice was made to have the domains as the dividing factor. The domains are based on the PoR[19], CPS[20], and PKIo hierarchy (internal document)[21]. The extended validation and public server domains are left out, as they are (soon to be) deprecated[22] [23]. The trustworthiness of the public and private root CAs inherit the risks from the intermediate domain CAs, as they are higher up in the PKI hierarchy. As the Private Person domain is not currently in use, analysing the private root CA is no more useful than analysing the Private Services domain. Therefore, the Private Person domain and private root CA will be left out of the analysis further on.

[15] https://www.logius.nl/diensten/digikoppeling/landelijke-voorzieningen
[16] https://certificaat.kpn.com/toepassingen/edsn/
[17] personal communication with a Logius employee
[18] https://cps.pkioverheid.nl/CPS_PA_PKIoverheid_G3_Root_v4.5.pdf, p. 9
[19] https://www.logius.nl/sites/default/files/public/bestanden/diensten/PKIoverheid/PoR-2022/PKIoverheid%20Programme%20of%20Requirements%20v4.10%20-%20Part%201%20Introduction.pdf, p. 22
[20] https://cps.pkioverheid.nl/CPS_PA_PKIoverheid_G3_Root_v4.5.pdf, p. 12
[21] PKIoverheid hiërarchie by Patrick van den Berg - 20210204
[22] https://www.logius.nl/actueel/pkioverheid-stopt-met-uitgeven-publiek-vertrouwde-webserver-ssltls-certificaten
[23] https://cert.pkioverheid.nl/

Step 3: Estimate impacts

Step 3.1: Estimate organisational impacts

The impacts of the threats from Step 1 on the assets of Step 2 are now assessed. First, the organisational impacts are assessed, meaning the impacts limited to the organisational scope. These are assessed for situations in which information security properties cannot be guaranteed for a business process. The information security properties are confidentiality, integrity, and availability.

Confidentiality:	property that information is not made available or disclosed to unauthorised individuals, entities, or processes.
Integrity:	property of accuracy and completeness.
Availability:	property of being accessible and usable on demand by an authorised entity.

To find the correct organisational impact scores, the table on page 8 is used. After filling in the scores, copy the highest score to the 'Total' column.

Table C.4: Step 3.1

Business process	CIA	Personnel	Capacity	Performance	Economic	Branding	Regulatory	Environment	Total
Trustworthiness assurance of the Organisation Person Domain	C	A	C	C	C	E	D	A	E
	I	A	C	D	C	E	D	A	E
	A	A	C	E	C	E	D	A	E
Trustworthiness assurance of the Organisation Services Domain	C	A	C	C	B	E	D	A	E
	I	A	D	D	C	E	D	A	E
	A	A	D	E	C	E	D	A	E
Trustworthiness assurance of the Citizen Domain	C	A	B	C	B	D	D	A	D
	I	A	B	D	B	D	D	A	D
	A	A	B	D	B	D	D	A	D
Trustworthiness assurance of the Autonomous Devices Domain	C	A	B	C	B	C	D	A	D
	I	A	B	D	B	C	D	A	D
	A	A	B	D	B	C	D	A	D
Trustworthiness assurance of the public root CA	C	A	D	C	C	E	D	A	E
	I	A	D	E	D	E	E	A	E
	A	A	D	E	D	E	E	A	E
Trustworthiness assurance of the Private Services Domain	C	A	B	C	B	D	D	A	D
	I	A	C	D	C	E	D	A	E
	A	A	C	E	C	E	D	A	E

Explanation: In general, no longer being able to guarantee confidentiality will hurt, but it will hurt Logius less than no longer being able to guarantee integrity or availability. Some use cases of certificates do not require confidentiality, only integrity and availability. Other use cases may prefer confidentiality but can continue without it guaranteed.

The capacity impact scores are estimated using the Logius year report numbers[24].

The usage of PKIo in the Organisation Person and Organisation Services Domains is more extensive than in the other two domains under the public root. Therefore, the branding impact scores will generally be lower. As expected, the public root security has the highest impact scores.

Table C.5: Organisational impact score card taken from SecRAM (Le Fevre et al., 2017)

Impact Areas	A No impact	B Minor	C Severe	D Critical	E Catastrophic
Personnel	No injuries	Minor injuries	Severe injuries	Multiple severe injuries	Fatalities
Capacity	No capacity loss	Loss of up to 10% capacity	Loss of 10% - 30% capacity	Loss of 30% - 60% capacity	Loss of 60% - 100% capacity
Performance	No quality abuse	Minor system quality abuse	Severe quality abuse that makes systems partially inoperable	Major quality abuse that makes major system inoperable	Major quality abuse that makes multiple major systems inoperable
Economic	No effect	Minor loss of income	Large loss of income	Serious loss of income	Bankruptcy or loss of all income
Branding	No impact	Minor complaints	Complaints and local attention	National attention	Government & international attention
Regulatory	No impact	Minor regulatory infraction	Multiple minor regulatory infractions	Major regulatory infraction	Multiple major regulatory infractions
Environment	Insignificant	Short term impact on environment	Severe pollution with noticeable impact on environment	Severe pollution with long term impact on environment	Widespread or catastrophic impact on environment

Step 3.2: Estimate societal impacts

This part of the assessment is done with a view that stretches further than the organisational scope. Here, the societal influence scope is applied. To get to the societal impacts, first the end-user impacts are assessed.

Step 3.2.1: Estimate end-user impact

Assess what the impact on end-users is if an information security property cannot be guaranteed anymore. This impact takes the form of a short-written answer in which the consequences for end-users are described.

Table C.6: Step 3.2.1

Business process	Trustworthiness assurance of the Organisation Person Domain	
Application	**CIA**	**Consequences for end-users**
Defensiepas	C	Military personnel cannot secretly share information anymore. Confidential military intel may leak.
	I	Hackers can forge military identities and intrude in buildings and ICT systems, which poses subsequent security risks. Fraud in immigrant processing is likely.
	A	There is no way for military personnel to communicate from outside closed networks. Immigrant processing will be much slower and with more room for fraud.
Personal UZI-pas	C	Highly sensitive health data of patients may leak.
	I	Hackers may alter health data resulting in wrong medicines or wrong medical procedures, hurting the health of patients, potentially killing them.
	A	Medical professionals (e.g., doctors) will not be able to communicate health data with each other efficiently, leading to long queues for medical care, possibly overflowing hospitals.
Taxi driver & inspector certificates	C	No impact, as there is no confidential data protected.
	I	This allows fraud and money laundering on an individual basis, as every individual certificate needs to be attacked.
	A	Taxi drivers will not be able to log their hours in a secure way and inspectors will not be able to audit the activities well. It will take more effort to do so for every individual driver and inspector, than it would be for whole taxi and inspection businesses.

Continued on next page

Table C.6 – *Continued from previous page*

Business process	Trustworthiness assurance of the Organisation Person Domain	
Application	**CIA**	**Consequences for end-users**
eHerkenning 4	C	Only select data can be leaked, as the lower tiers of eHerkenning are not affected.
	I	Only select data can be leaked, as the lower tiers of eHerkenning are not affected.
	A	Only select applications can be interrupted, as the lower tiers of eHerkenning are not affected.
Profession certificates	C	Businesses' financial documents communicated with/by accountants can be used for economic espionage. Some confidential legal communications with bailiffs might be illegally leveraged. It is not known whether notaries have confidential communications protected by PKIo.
	I	Digitally signed financial documents by accountants can be altered, opening a myriad of ways for large scale fraud (e.g., embezzlement). Judicial orders by bailiffs can be altered or fabricated obstructing justice or enabling fraud. For notaries there are opportunities to abuse fraudulent changes in databases of the Land Registry and Mapping Agency, the Chamber of Commerce and the Central Diploma Registry.
	A	Accountants, bailiffs, and notaries will be significantly hindered in their ability to perform parts of their jobs, as there is no way to perform legally binding actions digitally.

Explanation: Some applications see a breach in confidentiality where highly sensitive information is exposed. Other applications depend less on confidentiality and more on integrity. Compromises in integrity often lead to opportunities for (large scale) fraud. When availability cannot be guaranteed, attacks on specific individual cases can interrupt the services. There are ways thinkable in which the digital services can be replaced by non-digital alternatives, but these are much less efficient.

As these are personal certificates, relatively specific processes are heavily affected.

Table C.7: Step 3.2.1

Business process	Trustworthiness assurance of the Organisation Services Domain	
Application	**CIA**	**Consequences for end-users**
DigiD (organisation)	C	Sensitive citizen data such as financial-economic, religion, political preference, BSN, and health data will be leaked. As DigiD is widely adopted in the Netherlands, this will affect most citizens.
	I	Most public tasks concerning individual citizens can be heavily tampered with, enabling fraud and other malicious activities.
	A	Secure digital communication between citizens and governments is not possible, slowing down most public tasks immensely.
UZI-servercertificate	C	Highly sensitive health data of patients may leak.
	I	Hackers may alter health data resulting in wrong medicines or wrong medical procedures, hurting the health of patients, potentially killing them.
	A	Healthcare providers will not be able to communicate health data with each other efficiently, leading to long queues for medical care, possibly overflowing hospitals.
eHerkenning	C	Confidential data on businesses shared with a large amount of (semi-)governmental organisations can be leaked on a large scale. This includes financial data and personal data of employees.
	I	Many procedures that require contact between the market and (semi-)governmental organisations can be interfered with. Attacking a single organisation can already enable fraud on a large scale.
	A	The efficiency of procedures that require contact between the market and (semi-)governmental organisations can be heavily reduced, up to the point where the economy is significantly hurt.
eSeals	C	eSeals are not used for confidentiality. There is no impact.
	I	The purpose of eSeals is defeated. eSeals used in applications such as EPREL can be altered retrospectively. In the case of EPREL it means no energy label made in the past can be trusted anymore forever. Other applications are unknown.
	A	It is assumed that the checking of eSeals is the service of which availability is compromised. This means all eSeals lose their effect, as they cannot be verified. In the case of EPREL it means no energy label can be trusted as long as they cannot be checked. Other applications are unknown.

Continued on next page

Table C.7 – *Continued from previous page*

Business process	Trustworthiness assurance of the Organisation Services Domain	
Application	**CIA**	**Consequences for end-users**
Taxi business & inspection certificates	C	No impact, as there is no confidential data protected.
	I	This allows fraud and money laundering on a large scale, as entire businesses can be targeted.
	A	Taxi drivers will not be able to log their hours in a secure way and inspectors will not be able to audit the activities well. It will take less effort to do so for taxi and inspection businesses, than it would be for individual drivers and inspectors.
Explanation: The same conclusions on confidentiality, integrity, and availability from the Organisation Service Domain hold. The difference is as single certificates from the Organisation Service Domain are used for many transactions, the related impacts are broad affecting many cases at once. As these are non-personal certificates, more general processes are affected. There are broader impacts than with personal certificates, and although still heavy, less 'deep' impacts as opposed to the Organisation Person Domain.		

Table C.8: Step 3.2.1

Business process	Trustworthiness assurance of the Citizen Domain	
Application	**CIA**	**Consequences for end-users**
Vidua	C	Vidua is used for identification and signing. There are no consequences if confidentiality is broken.
	I	The possibility to alter housing, job, business, and other contracts signed with Vidua renders all contracts not legally binding. As Vidua is not widely adopted, impact will be relatively limited. Some companies will be more affected than others.
	A	Signing and identification through Vidua will not be possible anymore. As Vidua is not widely adopted, impact will be relatively limited. Some companies will be more affected than others.

Continued on next page

Table C.8 – *Continued from previous page*

Business process	Trustworthiness assurance of the Citizen Domain	
Application	**CIA**	**Consequences for end-users**
DigiD Substantieel & Hoog (citizen)	C	The highest tiers of DigiD are used to protect the most sensitive data. However, as attacks need to be done for individual citizen side certificates, more resources are required for attackers than attacking DigiD from the organisation side. This leaves highly sensitive personal citizen data at risk of leaking, but on a smaller scale than in the Organisation Services Domain. Additionally, lower DigiD tiers are unaffected.
	I	The same argument from above applies here.
	A	The most secure tiers of DigiD cannot be used anymore, but the argument above applies. Lower tiers can still be used, so the impact will be limited.
Explanation: Currently, Dutch society does not depend largely on certificates from the Citizen Domain. While there are alarming impacts for select cases, these do not affect the larger part of Dutch people.		

Table C.9: Step 3.2.1

Business process	Trustworthiness assurance of the Autonomous Devices Domain	
Application	**CIA**	**Consequences for end-users**
Taxi On-board Computer	C	No impact, as there is no confidential data protected.
	I	This allows fraud and money laundering on an individual basis, as every individual certificate needs to be attacked. However, the tampering with the identification of cars does not open up very easy and obvious ways for fraud.
	A	Taxi drivers will not be able to log their hours in a secure way and inspectors will not be able to audit the activities well. It will take more effort to do so for every individual on-board computer, than it would be for whole taxi and inspection businesses.
Explanation: The on-board taxi computer is the only application making use of the Autonomous Devices Domain. Even within the taxipas context the impacts in this domain are relatively limited.		

Table C.10: Step 3.2.1

Business process	Trustworthiness assurance of the public root CA	
Application	**CIA**	**Consequences for end-users**
Inherits all from previous four domains	C	Inherits all from previous four domains
	I	Inherits all from previous four domains
	A	Inherits all from previous four domains
Explanation: All four previous domains depend on the security of the public root CA. Therefore, all impacts in those four domains can materialise once the security of the public root CA is compromised.		

Table C.11: Step 3.2.1

Business process	Trustworthiness assurance of the Private Services Domain	
Application	**CIA**	**Consequences for end-users**
Digipoort	C	Tax reports, financial reports, and other potentially sensitive business information of involved parties may leak. Most of the Dutch market is not connected to Digipoort.
	I	Tax reports, financial reports, and other business communication to (semi-)government can be tampered with, creating opportunities for fraud.
	A	Previously automated messages have to be done by hand, creating large overhead for many companies and (semi-)governments.
Digikoppeling	C	Sensitive data from many different governmental databases can be captured.
	I	Data in many governmental databases can be tampered with opening options for fraud, but back-ups of this data should exist.
	A	Processes at (semi-)governments requiring data from external (semi-)governments will heavily slow down, as automatic data requests are not available.
ESDN	C	Some energy allocation data may be leaked, but it is assumed that this is not likely to heavily disturb the energy market.
	I	Tampering with automatic energy market processes is possible but is likely to be noticed.

Continued on next page

Table C.11 – *Continued from previous page*

Business process	Trustworthiness assurance of the Private Services Domain	
Application	**CIA**	**Consequences for end-users**
	A	Completely shutting down the electronic communication of the energy market will heavily disrupt it.

Explanation: There are likely to be more applications of the Private Services Domain, but these are out of sight of Logius. In these applications, tampering with the integrity again enables fraud. Compromising the availability will strain processes, hindering back-end systems, and creating overhead for the involved parties.

Step 3.2.2: Estimate impacts on national security

For each business process, fill in the table assessing the impact on national security a compromise of the applications related to the business process has. The scoring is done using the Leidraad risicobeoordeling Geïntegreerde risicoanalyse Nationale Veiligheid (GRNV). Use the results from Step 3.2.1 to help the scoring. After filling in the scores, copy the highest score to the 'Total' column.

Table C.12: Step 3.2.2

Business process	CIA	1.2 International position	1.3 Cyberspace	2.1 Deaths	3.1 Costs	3.2 Economy	5.1 Day-to-day life	5.2 Rule of law	Total
Trustworthiness assurance of the Organisation Person Domain	C	A	C	-	?	?	-	-	C
	I	A	C	B	?	?	-	A	C
	A	A	C	B	?	?	-	A	C
Trustworthiness assurance of the Organisation Services Domain	C	A	C	-	?	?	-	-	C
	I	A	C	B	?	?	-	B	C
	A	A	C	B	?	?	-	B	C
Trustworthiness assurance of the Citizen Domain	C	A	B	-	?	?	-	-	B
	I	A	B	-	?	?	-	A	B
	A	A	B	-	?	?	-	-	B
Trustworthiness assurance of the Autonomous Devices Domain	C	A	B	-	?	?	-	-	B
	I	A	B	-	?	?	-	-	B
	A	A	B	-	?	?	-	-	B
Trustworthiness assurance of the public root CA	C	A	C	-	?	?	-	-	C
	I	A	C	C	?	?	-	B	C
	A	A	C	C	?	?	-	B	C
Trustworthiness assurance of the Private Services Domain	C	A	B	-	?	?	-	-	B
	I	A	B	-	?	?	-	A	B

Continued on next page

Table C.12 – *Continued from previous page*

	A	A	B	-	?	?	-	A	B

Explanation:

1.2 It is difficult to judge the impact on the Dutch international position, as it may deteriorate because of other countries viewing Dutch cybersecurity as lacklustre. Following the description in the GRNV, cyberattacks and no other indicators lead to an impact score of A.

1.3 The deliverance of PKIo certificates is seen as an essential digital service. The following definition of domain size is used: the size of each domain is decided by the number of times a certificate in that domain is checked. As no data is currently available, the distribution is estimated based on the yearly report by Logius . It is then used to score impact area 1.3.

2.2 This impact area is relevant because of the UZI-registry. Effects in one of the two domains involving the UZI-registry can partially be relieved by using the certificates from the other domain. However, when both domains are affected through the root CA, heavier impacts will be felt. The death counts and related impact scores are estimated.

3.1 and **3.2** Both of these impact areas involve estimations that I have no experience with. I imagine that breaches concerning the Organisation Services Domain and especially the public root CA will have the highest impact scores.

5.1 There are ways in which daily life is affected by making digital communication, especially with the government, hard. However, when examining the six indicators in the GRNV, none apply.

5.2 The functioning of public administration is the one criterion that matters in the context of this assessment. While confidentiality is important, it is not necessary for the functioning of public administration with the systems considered. The difference between the Organisation Person and Organisation Service domains is because of the estimated part of public administration to be affected. As for the Citizen Domain, when integrity is compromised, this could hinder public administration significantly. However, when there are enough alternatives so that a compromise of availability would not result in a significant disruption.

Step 4: Estimate likelihood

Because it is uncertain when a large enough quantum computer will be available, in this step the time to act is approximated. To do so, the following variables are estimated for each business process.

X =	longest shelf life of data within the scope of the business process [years]
Y =	time it will take to replace all vulnerable cryptography used within the scope of the business process to quantum safe cryptography [years]
Z =	estimated time until a powerful enough quantum computer is available [years] (may vary depending on risk appetite)
t =	theoretical time to act [years]

The resulting theoretical time to act (t) is not an exact figure and should not be interpreted as such. It is based on three estimates and is therefore an approximation.

Table C.13: Step 4

Business process	X	Y	Z	**Threat**	**Formula for t**	t
Trustworthiness assurance of the Organisation Person Domain	20	10	18	Real-time access (CIA)	t = Z – Y	8
				Store now, decrypt later (C)	t = Z – X – Y	-12
Trustworthiness assurance of the Organisation Services Domain	20	10	18	Real-time access (CIA)	t = Z – Y	8
				Store now, decrypt later (C)	t = Z – X – Y	-12
Trustworthiness assurance of the Citizen Domain	15	10	18	Real-time access (CIA)	t = Z – Y	8
				Store now, decrypt later (C)	t = Z – X – Y	-7
Trustworthiness assurance of the Autonomous Devices Domain	5	10	18	Real-time access (CIA)	t = Z – Y	8
				Store now, decrypt later (C)	t = Z – X – Y	3
Trustworthiness assurance of the public root CA	20	10	18	Real-time access (CIA)	t = Z – Y	8
				Store now, decrypt later (C)	t = Z – X – Y	-12
Trustworthiness assurance of the Private Services Domain	10	10	18	Real-time access (CIA)	t = Z – Y	8
				Store now, decrypt later (C)	t = Z – X – Y	-2

Explanation: The variable Z is constant. In this assessment, the assumed time until a quantum computer is available is 20 years from 2020, so 18 years from now[25].

The variable Y is based on personal communication with a Logius employee, stating that replacing all PKI cryptography is likely to take 10 years.

Variable X is about data shelf-life. Medical dossiers are to be kept for 20 years in most cases[26]. Currently most governmental information considered classified is kept secret for 20 years[27]. There is no clear guideline on how long personally identifiable data should be kept secret. Ideally, it is kept secret indefinitely. The same holds true for medical dossiers. However, for the purpose of analysis, 15 years is chosen. The data used for cab fares that makes use of the Autonomous Devices Domain is not relevant for a long time, and thus 5 years is chosen as the shelf-life. In case of the Private Services Domain, a value of 10 years is chosen, as the government databases in question are not public, but the data is not highly confidential and changes over time.

Step 5: Combine results

The results from all previous steps are combined in a single table. The organisational and national impact are taken from Steps 3.1 and 3.2.2 respectively. The theoretical time to act (t) is taken from Step 4. Lastly, using the conversion matrix, the risks can be ranked. Taking the highest of the two impact scores and the theoretical time to act, the matrix ranks the risk for each threat to each business process. It should be noted that the conversion matrix can be adjusted according to the risk appetite of the assessing organisation.

Table C.14: Step 5 overview

Business process	**Threat**	**Organisational impact**	**National impact**	t
Trustworthiness assurance of the Organisation Person Domain	Real-time access (CIA)	E	C	8
	Store now, decrypt later (C)	E	C	-12
Trustworthiness assurance of the Organisation Services Domain	Real-time access (CIA)	E	C	8
	Store now, decrypt later (C)	E	C	-12
Trustworthiness assurance of the Citizen Domain	Real-time access (CIA)	D	B	8
	Store now, decrypt later (C)	D	B	-7
Trustworthiness assurance of the Autonomous Devices Domain	Real-time access (CIA)	D	B	8
	Store now, decrypt later (C)	D	B	3
Trustworthiness assurance of the public root CA	Real-time access (CIA)	E	C	8
	Store now, decrypt later (C)	E	C	-12
Trustworthiness assurance of the Private Services Domain	Real-time access (CIA)	E	B	8
	Store now, decrypt later (C)	D	B	-2

Table C.15: Step 5 conversion matrix

Impact score	t			
	> 5	$4 - 0$	$-1 - -5$	< -5
A	Acceptable	Acceptable	Moderate	Moderate
B	Acceptable	Acceptable	Moderate	Severe
C	Acceptable	Moderate	Severe	Severe
D	Moderate	Severe	Severe	Critical
E	Severe	Severe	Critical	Critical

Table C.16: Step 5 synthesis results

Business process	**Threat**	**Risk category**
Trustworthiness assurance of the Organisation Person Domain	Real-time access (CIA)	Severe
	Store now, decrypt later (C)	Critical
Trustworthiness assurance of the Organisation Services Domain	Real-time access (CIA)	Severe
	Store now, decrypt later (C)	Critical
Trustworthiness assurance of the Citizen Domain	Real-time access (CIA)	Moderate
	Store now, decrypt later (C)	Critical
Trustworthiness assurance of the Autonomous Devices Domain	Real-time access (CIA)	Moderate
	Store now, decrypt later (C)	Severe
Trustworthiness assurance of the public root CA	Real-time access (CIA)	Severe
	Store now, decrypt later (C)	Severe

Explanation: Using the conversion matrix, we come to these risk categories for each business process. The interpretation of these risks is further detailed in Chapter 5