Master's Thesis

Information security certification in context: a strategy selection maturity model

Mike Hulshof (s1737112)
Master of Science Business Information Technology
Specialization Enterprise Architecture & IT Management
Faculty of Electrical Engineering, Mathematics
and Computer Science (EEMCS)

m.hulshof@alumnus.utwente.nl

Supervisors:
Innovalor – Dr. Bob Hulsebosch
University of Twente – Dr. Maya Daneva
University of Twente – Dr. Adina Aldea

August 2021

UNIVERSITY OF TWENTE.

Executive Summary

For the last 20 years, increasing globalization and technological development have enabled and stimulated a greater degree of outsourcing smaller IT sub-components to more specialized vendors. The shift from an industry characterized by in-house development with little use of outsourcing to an industry with less in-house development and more widespread use of outsourcing has introduced novel challenges for technology providers worldwide. Technology providers, tasked with the development and delivery of these outsourced sub-components, must earn the trust of their partners by showing that they operate securely. Many organizations earn this trust through the assurance from an independent party, often in the form of security certification. However, traditional certification schemes are not catered to the use of widespread outsourcing and sub-contracting, introducing challenges for technology providers that must adhere to these schemes.

This master's thesis is carried out in cooperation with Innovalor, a technology provider specialized in the field of identity proofing and investigated information security certifications in the context of technology providers. The objective of this research project is to develop an artifact that supports the selection of an effective information security certification strategy. To this end, this master's thesis is structured according to the Design Science Research Methodology (DSRM) and consists of three phases: Problem investigation, treatment design and treatment validation.

In the **problem investigation phase** an extensive problem analysis was performed. First, a systematic literature review was conducted on the value of information security certification. Next, qualitative interviews with three stakeholders within Innovalor were conducted, revealing practical challenges associated with information security certification and establishing initial treatment candidates. These findings were compared to the findings from the literature review to reveal similarities and discrepancies between theory and practice. Subsequently, in addition to the interviews, several existing treatment candidates were extracted from practical developments in the field of information security certification.

In the **treatment design phase** the artifact of this research project was designed. First, based on the findings from the first phase (problem investigation), the notion of a technology provider certification lifecycle was introduced. This model provides a general representation of the different stages of certification based on four scenarios. Second, additional qualitative interviews were conducted with eighteen stakeholders from several areas related to information security certification. The participants were asked to reflect on the treatment candidates that emerged from the problem investigation phase and they were given the opportunity to contribute with strategies of their own. All stakeholders were experts in their respective fields, providing a multidisciplinary perspective. From these interviews, five certification strategies and four optimization practices emerged, which led to the construction of a certification strategies selection framework. Finally, the selection framework was expanded to include optimization of one's information security certification processes within a given scenario, which was accomplished by incorporating the concept of dedicated maturity levels into the construction of a novel certification maturity model. This certification maturity model forms the artifact of this research project and is designed to be used in a prescriptive manner. The model serves two purposes:

- First, it aids in the construction of a development roadmap by showing how the maturity of information security certification strategies can be improved to positively affect the value of the business and/or processes.
- Second, it can help in the decision-making process when considering an appropriate strategy for acquiring new certifications and managing existing ones, based on the context in which a technology provider operates.

In the **treatment validation phase** the certification maturity model was validated according to the Unified Theory of Acceptance and Use of Technology (UTAUT). Expert interviews were conducted, in which the certification maturity model was submitted to a panel of nine experts from varying backgrounds. These experts were asked to predict what effects they think the proposed solution would have if it would be implemented in practice. Based on the findings of the validation, it was concluded that (1) the artifact sufficiently and accurately represents reality, (2) provides guidance when selecting an appropriate information security certification strategy by facilitating the construction of a certification roadmap and (3) the artifact itself is both easy to use and useful to Innovalor and practitioners from the field.

The main strengths of this research are the introduction of the certification strategy selection framework and the certification maturity model. To conclude, the contributions of this research are fivefold:

1. By visualizing a high-level overview of the certification process based on the literature.
2. By visualizing the information security certification landscape from the perspective of Innovalor.
3. By introducing the notion of a technology provider certification lifecycle, showing the variability in certification needs as a technology provider progresses through four possible scenarios.
4. By constructing a certification strategies selection framework, mapping the strategies onto the same scenarios introduced in the technology provider certification lifecycle.
5. By combining the previous findings to construct an information security certification maturity model.

Future work can improve on the limitations of this research project. The artifact could potentially be expanded to promote generalizability outside the field of information security certifications (e.g. certifications in general), across a broader context (e.g. outside of Europe) or beyond the scope of technology providers (e.g. outsourcing in general). In particular, we hypothesize that outsourcing of generic sub processes in general could be considered as a candidate scope in future research, but this requires further evaluation. The field of information security certification and IT auditing is continuously evolving, which puts the artifact presented in this research project at risk of becoming outdated if it is not revised to keep up with the developments. Finally, future research would do well to closely monitor and evaluate the ongoing developments concerning a modular approach to certification. Of particular interest are the ETSI standards that are continuing to emerge, which cater to the practical application of component certification.

Preface

This Master's thesis marks the end of my five-year journey at the University of Twente. At the beginning of this journey, I enrolled in the Bachelor's degree of Business Information Technology at the Faculty of Electrical Engineering, Mathematics and Computer Science (EEMCS). Upon graduating from the Bachelor's degree, I was left puzzled. I did not even have the faintest idea on what type of career I wanted to pursue. Thus, I quickly settled on the idea of buying myself some more time and opted to first pursue the subsequent Master's degree in the same field of Business Information Technology (BIT). Luckily, this choice panned out well, because it coincidentally gave me the opportunity to gain a number of priceless experiences that I had not foreseen prior to enrolling in the Master's degree. I would like to take this opportunity to share one particular life-changing event with the reader of this dissertation.

During my Master's degree, I had the opportunity to attend a six-month study abroad exchange program at Waseda University in Tokyo, Japan. Throughout that period, I experienced a culture vastly different from the Netherlands in any way imaginable. I was put in an environment where I knew nobody, barely spoke the local language and had to learn Japanese etiquette from scratch. However, by the end of the exchange I had forged some of the best friendships of my life, was capable of basic communication in the local language and had discovered a newfound admiration for the Japanese culture. Japan had become my new home and when the exchange finally ended, I was reluctant to return to the Netherlands. This rather short six-month study abroad allowed me to undergo more social development than the last four years prior to the exchange combined. I cannot put into words how valuable this experience was and it ignited a passion inside of me to make a career in Japan in the future. Throughout this graduation project, I have kept up my Japanese studies in in the hope of one day achieving that goal.

I have always had an interest in IT auditing, because it forms the bridge that unites the technical side of IT with the business related aspects of compliance. IT auditors apply their professional judgement on a case-by-case basis to strike a balance between compliance for the sake of compliance on the one hand and inadequate risk assurance on the other hand. This resonates with me, because the BIT program is centered around educating students on becoming the bridge between business and IT. Innovalor provided me with the opportunity to contribute to this field by conducting research on information security certifications. I particularly enjoyed getting to interview genuine experts from the field. Given the complexity of the subject matter at hand, condensing the sometimes seemingly contradictory responses among the experts into a concise and scientifically sound thesis was challenging to say the least. However, as challenging as it might have been, it was an incredibly rewarding experience and I am pleased to say that I am satisfied with the result.

The graduation project took place in quite the peculiar setting. The entire research project was conducted in the middle of the lockdown during the Covid-19 pandemic. Physical presence at the office was restricted to the bare minimum and capped at no more than once weekly. All communication with the theoretical supervisors was done digitally from home. As the project approached its deadline, we were faced with a nerve-wracking challenge. Due to unforeseen circumstances, the original second supervisor had to put a pause on the supervisory process. Luckily, we were able to make some last-minute adjustments that resulted in a sudden change in the supervisory process.

I would like to take this opportunity to express my gratitude to some of the great people who supported me throughout the project. From Innovalor, I would like to thank Bob Hulsebosch as the practical supervisor for this graduation project. Bob's extensive experience in the field and willingness to engage in open discussions were invaluable to the success of this project. From the University of Twente, I would like to thank Maya Daneva, Adina Aldea and Victoria Daskalova for their guidance as theoretical supervisors. Their feedback from a theoretical perspective was complementary to Bob's feedback from a practical perspective. Finally, I would like to thank all 21 interview participants for their participation and insightful responses. All of them were a tremendous help and I am incredibly grateful that they were willing to free up their valuable time. Without their cooperation, it would not have been possible to conduct this research.

I now happily invite you to read the thesis and hope that you will find it interesting or useful.

Mike Hulshof

Contents

List of Figures

List of Tables

List of Abbreviations

AML: Anti Money Laundering
AWS: Amazon Web Services
BIG: Baseline Informatieveiligheid Gemeenten
BIO: Baseline Informatiebeveiliging Overheid
CEO: Chief Executive Officer
CMM: Capability Maturity Model
COBIT: Control Objectives for Information and Related Technologies
DNB: De Nederlandsche Bank
DSRM: Design Science Research Methodology
EGiZ: Gedragscode Elektronische Gegevensuitwisseling in de Zorg
eIDAS: electronic Identification, Authentication and trust Services
ENISA: European Union Agency for Cybersecurity
ENSIA: Eenduidige Normatiek Single Information Audit
ETSI: European Telecommunication Standards Institute
GRC: Governance, Risk & Compliance
IRM: Integrated Risk Management
ISAE: International Standard on Assurance Engagements
ISMS: Information Security Management Systems
ISO: International Organization for Standardization
NFC: Near Field Communication
RvA: Raad van Accreditatie
SDK: Software Development Kit
SME: Small and Medium-Sized Enterprises
SOC 2: Service Organization Control 2
TAM: Technology Acceptance Model
TPM: Third Party Memorandum
TSP: Trust Service Providers
UTAUT: Unified Theory of Acceptance and Use of Technology
WWFT: Wet ter Voorkoming van Witwassen en Financieren Terrorisme

1 Introduction

For the last 20 years, increasing globalization and technological development have enabled and stimulated a greater degree of outsourcing smaller IT sub-components to smaller, more specialized vendors [1]. Rather than relying on in-house development, organizations now tend to utilize the expertise of several partners to optimize their processes. The shift from an industry characterized by in-house development with little use of outsourcing to an industry of widespread use of outsourcing with less in-house development has introduced novel challenges for technology providers worldwide. Nowadays, banks tend to stick to their core financial practices whilst outsourcing technical parts of the process to numerous IT suppliers. Hospitals tend to be predominantly occupied with providing medical healthcare by utilizing a combination of in-house development and outsourced IT to support their primary tasks. Even among organizations that supply IT products and/or services, it is becoming more common to utilize outsourced components for specific parts of the development of the product or service itself [2].

Technology providers, tasked with the development and delivery of these outsourced sub-components, must earn the trust of their partners by showing that they operate securely. There is more than one way in which this can be achieved, but one of those methods is the widely adopted process of certification, often given out by an independent third party. This thesis investigates information security certification strategies and maturity models for technology providers that are active in multiple sectors and industries.

The remainder of this chapter introduces the research topic of this thesis. Section 1.1 defines the context in which this research is carried out. Section 1.2 defines the core concepts and definitions. Section 1.3 describes the research problem, followed by the goal of the research in section 1.4. Section 1.5 introduces the research questions. Finally, the chapter concludes by providing an outline of the structure of the paper in section 1.6. In preparation for this Master's thesis, the author of this research conducted a systematic literature review prior to the start of this research [3]. In order to not self-plagiarize, we take this opportunity to inform the readers that the introduction and background chapters contain body of text taken directly from the literature review. In this chapter, section 1.1, 1.2 and 1.3 contain parts from the literature review.

1.1 Context

This research is performed in cooperation with Innovalor, a startup IT and consulting company of roughly 40 employees located in Enschede. They offer a combination of advisory services and software solutions. One of their products is ReadID, a piece of software that provides identity data and document verification using a mobile app and Near Field Communication (NFC) technology to read the data from chips on identity documents such as passports, driver's licenses, or ID cards. Through this, they can remotely verify the authenticity of the data and the documents themselves.

The ReadID solution is provided by Innovalor to customers as a mobile software development kit (SDK) or as a ready-to-use app in combination with a server that performs all the verifications and is hosted by a public cloud provider. However, these customers are active in different sectors and industries, most of which demand that Innovalor must be certified with the same information security certifications as the customers. As a result, Innovalor is expected to be certified for or be compliant with (often nearly identical) sector-specific information security standards that are costly and require periodic, recurring IT audits (often initiated by their customers). Furthermore, the abundance of information security frameworks and standards adds to the complexity [4], with over 180 published cybersecurity standards in various languages, sectors and countries [5].

For example, when a person wishes to borrow capital from a bank, a bank goes through an extensive process prior to providing the loan. This process includes the identity authentication of their client, which can be outsourced to partners such as Innovalor. Innovalor verifies the identity and validates the client's documents. However, to perform the verification, they outsource part of their own process to partners such as subcontractors and public cloud providers. The bank then requires Innovalor (and its partners) to be certified for or be compliant with certain information security certifications.

1.2 Concepts & Definitions

The general concept of certification is defined as *"the action or process of providing someone or something with an official document attesting to a status or level of achievement"* (Oxford Dictionary[1]). Security certification revolves around three concepts, namely assessing whether the internal control measures are designed and documented properly, whether they are implemented and whether they are working effectively (in Dutch, these refer to the concept of opzet, bestaan en werking). Given the abundance of information security standards, many different frameworks and certifications have developed over the years. These security standards and certifications can differ in terms of scope, depth and even the type of audit.

One can distinguish between organizational security certifications and product certifications. Organizational certifications are wider in scope and applicable to organizations regardless of the industry in which it operates. These certifications often allow the auditee to determine the applicable areas of a security standard by specifying the scope for which they wish to be certified. Furthermore, organizational certifications often permit the construction a statement of applicability to define which controls are relevant. Examples of organizational certifications are ISO 27001, SOC 2 and NEN 7510. We would like to take this opportunity to inform the readers that SOC 2 is technically not a certification, but an assurance report. However, in practice many technology providers consider SOC 2 interchangeable with other information security certifications. Therefore, in this research, we consider SOC 2 to be comparable with organizational certifications in the sense that it can be applicable to organizations as a whole and allows a high degree of freedom when constructing the scope. Product certifications on the other hand are narrower in scope, but larger in depth. These types of certifications provide assurance on a specific type of product or service and tend to be utilized in sector-specific contexts. Examples of such certifications are PCI DSS in the financial sector, FIPS 140-2 for hardware security modules or the standards developed by the European Telecommunication Standards Institute (ETSI) for trust service providers (TSPs). However, the latter category of standards (ETSI) contains aspects of both the product and relevant processes.

Irrespective of certification type, some standards allow for the use of component certification (sometimes also referred to as module certification). In practice, this currently occurs in two ways. First, it is possible for standards to extend each other, often through additional controls in specific areas on top of existing standards. This phenomenon occurs with many ISO (International Organization for Standardization) standards, where the earlier-mentioned ISO 27001 acts as an organization-wide security baseline, which can be extended by other standards such as ISO 27002, ISO 27701 (privacy focus) or ISO 27017 (cloud focus). The second way in which component certification is currently utilized can be seen in some of ETSI's standards, which has split its standards into smaller individual components, allowing organizations to acquire certifications for smaller sub-components for the specific area in which they operate. Although these two types differ slightly, the core concept of component certification is that a common baseline is extended with narrower, but more specific set of controls in the relevant areas to reduce audit overhead. The emphasis here is that a component certification extends, but not replicates, existing certification.

Information security certifications are provided through a process known as *IT auditing*, which does not have a unanimous definition according to the literature. We have chosen to adopt the definition used by Aditya et al. (2018), where IT auditing is defined as a *"systematic, independent and objective process of assurance that is conducted periodically and in accordance with standards, so as to provide reasonable assurance and a continuous improvement of a successful IT implementation*" [6]. Many industries have undergone digital transformations, increasing the demand for IT audits [7]. A more elaborate analysis of the certification process and its relevant stakeholders will be provided in section 2.1 of this research.

For the purpose of clarity, we add an explanation of how the term certification and IT auditing relate to each other. In practical terms, certification often entails a document that provides assurance by an independent and accredited third party that an organization is operating conform a certain security standard. If the goal is to acquire a certification, then we follow the process of IT auditing to acquire said certification. However, the concept of auditing is not unique to the field of information security. IT auditing or auditing in general, can also be applied to goals other than the acquisition of IT security

[1] https://www.lexico.com/definition/certification

certifications. It can be any type of certificate, such as quality management, sustainability or even a financial certificate.

1.3 Problem Statement

Besides the growth of IT outsourcing, numerous industries have developed their own information security related certifications, often driven by sector-specific regulation. Most sectors have their own supervisory regimes such as the DNB (De Nederlandsche Bank[2] or *Dutch Federal Bank* in English) for the Dutch financial sector, the Nationale Zorgautoriteit[3] (*National Health Authority* in English) for the Dutch healthcare sector, or the Agentschap Telecom[4] (*Radio Communication Agency* in English) for trust service providers issuing digital certificates under the EU eIDAS regulation. These authorities set requirements and standards, often driven by the extremely sensitive nature of the data being processed, based on sector-specific regulations such as:

- AML[5] (anti-money laundering) regulation for the financial sector.
- The EGiZ Gedragscode[6] (Gedragscode Elektronische Gegevensuitwisseling in de Zorg or *code of conduct for electronic data exchange* in English) in the healthcare sector.
- The EU eIDAS (electronic Identification, Authentication and trust Services) regulation for trust service providers in Europe [8].

As a result, different industries utilize their own certifications, which have developed over the years and may share similarities across different sectors. Although often not explicitly stated in the regulation themselves (at least not in the Netherlands), they practically indirectly require demonstrable compliance in the form of certification [4]. In turn, when these organizations outsource parts of their processes, their outsourcing partners must demonstrate compliance with the same standards as well. For example, according to the DNB (financial sector) an ISO 27001 certificate insufficiently checks whether controls have been successfully implemented in practice. Instead, the Dutch financial sector gravitates towards SOC 2 assurance reports. For the Dutch healthcare sector a typical mandatory certification is the NEN 7510, which is nearly identical to ISO 27001 and only contributes with a handful of additional healthcare-specific controls. In other words: There is no certification that covers them all.

This situation of IT outsourcing in combination with compliance to regulation and supervisory bodies leads to new challenges for technology providers that are active across multiple sectors. In the absence of an extensive track record, organizations rely on certifications to build trust and credibility. Therefore, it is unsurprising that many businesses require their partners to adhere to the same standards to be eligible to engage in a trustworthy and responsible partnership.

The continuous auditing demands can result in cumbersome situations when IT companies that desire to cooperate with partners from various industries are expected to comply with their potential partners' (perhaps nearly identical) sector-specific information security standards. For example, TSPs often require certain ETSI standards, financial institutions demand a SOC 2 assurance report and healthcare providers want to see NEN 7510. Auditing overhead can be particularly troublesome for collaborating SMEs (Small and Medium-Sized Enterprises), who lack the resources and capital required to fund the acquisition of these many certifications and subsequent continuous IT audits. Particularly, major overlap among certifications may unnecessarily inhibit innovation through certification entry-barriers, because SMEs may not be able to meet the capital demands required to accommodate the information security certifications or IT audits to such an extent.

This research project investigates certification strategies that allow technology providers, such as Innovalor, to engage in partnerships without the unrealistic expectation of enduring continuous IT audits and having to allocate a significant number of resources to facilitate these. Acquisition and maintenance of information security certifications is expensive and IT audits are time-consuming from both an

[2] https://www.dnb.nl/
[3] https://www.nza.nl/
[4] https://www.agentschaptelecom.nl/radiocommunications-agency
[5] https://www.lexisnexis.nl/kennisbank/themas/aml
[6] https://www.knmg.nl/web/file?uuid=fd2e8f1b-b0ac-4b78-85d3-a09d2ce00e06&owner=5c945405-d6ca-4deb-aa16-7af2088aa173&contentid=78264

administrative perspective, as well as the necessity to dedicate human resources towards the accommodation of on-site IT auditor visits. These sector-specific certification demands can result in situations in which more or less duplicate audits are imposed that may add little to no value on top of existing certification. This research project focuses on *four concrete challenges* that Innovalor faces regarding information security certification:

First, customers outsource a small part of their processes to Innovalor, namely the identity verification part of the process. As such, whenever a customer is audited, Innovalor is audited as well. Therefore, if many similar customers are audited, Innovalor will have to endure continuous audits proportionate to the number of audits which their customers are subjected to. The only way to alleviate the burden of these time-consuming audits is to acquire adequate certification, which requires a single audit effort, provides reasonable assurance and mitigates the necessity for multiple other customer audits due to its reusability.

Second, as a technical solution provider Innovalor has many different types of customers across various sectors or industries, such as TSPs, banks, healthcare providers and even governmental organizations. Many of them have their own audit demands, which Innovalor must adhere to. As such, different customers demand different types of certifications. Whereas one customer may demand a SOC 2 assurance report, another party might only accept ETSI certification. The sector-specific nature makes it difficult to utilize the same information security certification across multiple sectors. Regardless of the existing certification's similarity in scope and level of assurance, many customers only accept those that meet their own specific audit demands. Moreover, regulation and geographical factors also play a role as well. Due to regulatory differences, the commonly adopted information security standards in the United States are different from Europe.

Third, for the development of their services (identity verification), Innovalor cooperates with other parties, such as subcontractors and public hosting providers. When operating in an environment where information security certification is considered important, the communication between the involved chain of parties can become complex. When trying to integrate different certifications, how can we ensure that the communication and interaction between those parties are sufficiently guaranteed even if they are certified individually? Certifications provide assurance within a given scope, but often do not consider integration between different certification schemes.

Fourth, Innovalor itself is not a financial service provider, healthcare service provider or trust service provider. Innovalor merely provides a small technological IT component for these parties. In turn, it does not make sense for them to meet all the security controls that a bank, healthcare provider or trust service provider must comply with. Typically, Innovalor only has to comply with a subset of the controls and not all certification schemes cater for this.

To summarize, the four main problems are as follows:

1. Whenever a customer is audited, Innovalor is also audited.
2. Customers often have their own accepted vendor certifications.
3. Integration between different certification schemes is complex and error prone.
4. Full certification may not be necessary.

To illustrate the problems outlined above, Figure 1 provides a schematic overview of the described problem scenario. A step-by-step explanation through the diagram from top to bottom is provided below.

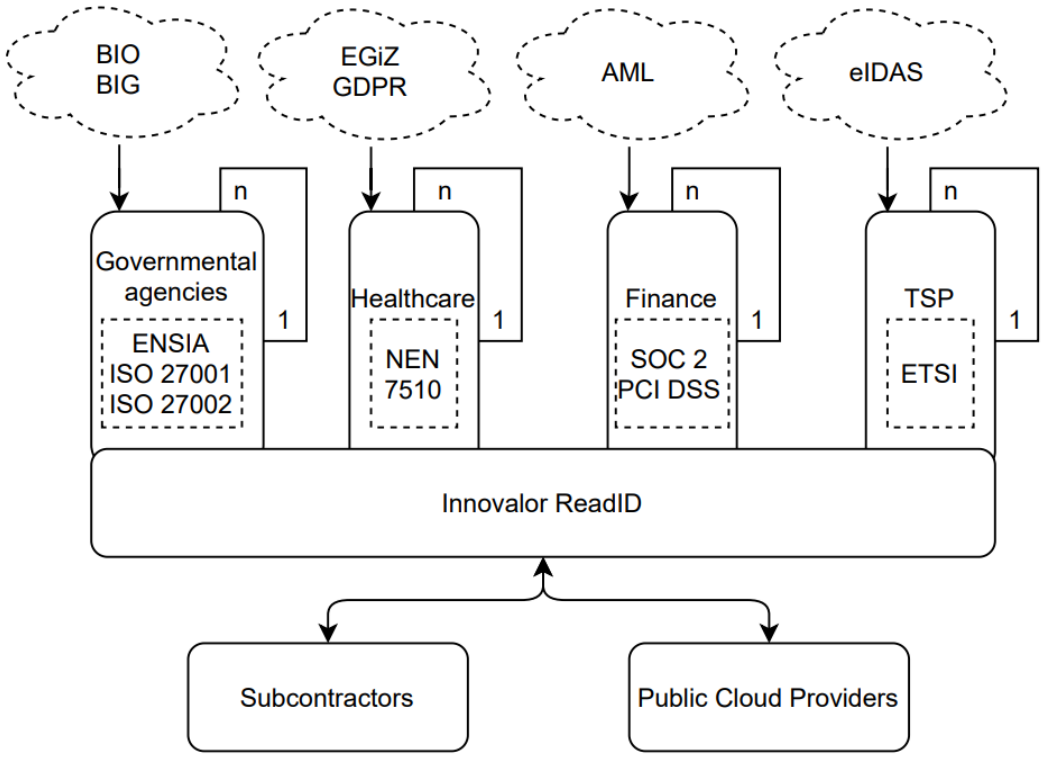

Figure 1: Schematic overview of the current situation.

The top of the figure displays some of the potent driving forces in the form of regulation behind the adoption of sector-specific certifications, depicted by the cloud-shaped objects in Figure 1 (regulatory requirements). As mentioned in the first paragraph of this section, regulation promotes the use of certification, because organizations are required to show an adequate level of protection conforming regulation. Although certification is not explicitly required, in practice, compliance is often expressed through information security certification.

In Figure 1, the vertical rectangles below the clouds represent the sectors in which Innovalor operates. Different sectors develop their own certifications with varying degrees of differences. Moreover, depending on the scope of a certification within a given context, it is possible that certain sector-specific certifications provide nearly identical levels of assurance. Inside of these sectors, depicted by the dotted lines, are the sector-specific standards. From these standards, ENSIA (Eenduidige Normatiek Single Information Audit) warrants some additional explanation as it has not been mentioned thus far. ENSIA describes a process that applies to governmental agencies and aims to develop and implement a single information audit method for information security[7]. More information on ENSIA will be given in section 2.3.3.

Innovalor is represented by the horizontal rectangle that overlaps with vertical rectangles of the sectors Figure 1. Innovalor's scope is rather narrow (identity verification) and they are only responsible for a small subset of the customers' processes, hence they only play a minor part in many different sectors. Even though Innovalor only plays a minor role, they are still required to adopt the different sector-specific certifications if they wish to reduce the demand for continuous extensive IT audits.

Lastly, Innovalor's partners are located at the bottom of Figure 1. For the development of ReadID, Innovalor outsources biometrics to a subcontractor and server hosting to public cloud providers. When one of these parties is audited, the others are also subjected to an audit. These parties can acquire appropriate certification to avoid or mitigate the audit overhead.

[7] https://www.ensia.nl/#!/

1.4 Research Goal

Based on the four challenges defined in the previous section, the overall objective of this research project is to establish effective strategies for technology providers to satisfy the (often sector-specific) information security requirements of customers or their supervisory bodies. In addition, this research assesses the feasibility of different strategies for reducing the audit overhead and aid technology providers in the decision-making process. In line with this, the research goal of this master project is:

To design and validate an artifact that treats the challenges associated with information security certification by supporting technology providers in choosing an effective information security certification strategy.

1.5 Research Questions

As explained in the previous section, the goal of this research is to support technology providers in choosing an effective information security certification strategy in order to ease up on the information security certification demands. As such, this leads us to the following **main research question**:

Given the complexity of information security certification, what are effective strategies for technology providers to satisfy sector-specific information security demands?

To aid with answering the main research question, the following sub-questions were constructed:

RQ1: *What challenges do technology providers face regarding information security certifications?*

RQ2: *What are the current common practices of information security certification?*

RQ3: *What strategies and maturity models exist for effectively satisfying information security demands through certifications?*

RQ4: *What are the advantages and disadvantages of the different strategies?*

RQ5: *What are the factors that influence strategy selection?*

RQ6: *What is the applicability of the proposed artifact?*

- **RQ6.1:** *To what extent is the proposed artifact useful to practitioners in the field?*
- **RQ6.2:** *To what extent is the proposed artifact usable by Innovalor?*

1.6 Research Outline

A research framework was constructed to address the research question introduced in the previous sub-section (depicted below in figure Figure 2). This research project consists of three phases: (1) problem investigation, (2) treatment design and (3) treatment validation.

Chapter 2 covers the relevant theoretical and practical background on the topic of information security certification and the field of IT auditing. Section 2.1 explains the information security certification process is explained in detail. Section 2.2 summarizes the conclusions of the systematic literature review, which was conducted by the author of this thesis as part of the research topics paper in preparation for the research project and investigated the value of information security certification. Section 2.3 concludes the background chapter by presenting relevant practical developments in the field of information security certification.

Chapter 3 covers the research methodology. Section 3.1 introduces the methodology of this research project, namely the Design Science Research Methodology (DSRM) developed by Wieringa [9]. DSRM follows the design cycle and consists of three phases: (1) problem investigation, (2) treatment design and (3) treatment validation. Section 3.2 presents the approach to the collection and analysis of data. Section 3.3 presents the approach to the problem investigation phase, which investigates potential existing treatments from the literature (which is covered in chapter 2) and performs a problem analysis. Regarding the problem analysis, a stakeholder analysis is performed according to the DSRM's stakeholder taxonomy. In addition, the process for conducting qualitative interviews with stakeholders within Innovalor is described in order to identify practical challenges associated with information security certification. Section 3.4 presents the treatment design phase, which describes the process for

conducting qualitative interviews with stakeholders outside of Innovalor to design an artifact that can solve the identified challenges. Section 3.5 concludes the methodology chapter and explains the process for validating the proposed artifact through expert evaluation, based on an adaptation of the technology acceptance model (TAM).

Chapter 4 covers the results and consists of two parts. Section 4.1 presents the results of the *problem investigation* phase. First, the findings of the qualitative interviews conducted within Innovalor are presented. These practical interview findings are then analyzed and compared to the theoretical findings of the literature review. Section 4.2 presents the results of the *treatment design* phase. First, a novel model called the technology provider certification lifecycle is introduced, which was constructed based on the results of the interviews for both the *problem investigation* phase and the *treatment design* phase. Afterwards, five certification strategies and four general optimization practices are presented. Finally, the chapter concludes by introducing a novel strategy selection framework, in which these nine concepts (five strategies and four optimization practices) are mapped onto one cohesive framework.

Chapter 5 covers the concept of *maturity models* and presents the artifact of this research project. Section 5.1 provides relevant theoretical background information on the topic of maturity models. Section 5.2 introduces a novel certification maturity model, which forms the artifact of this research project. This certification maturity model is an extension of the selection framework introduced at the end of chapter 4.

Chapter 6 covers the treatment validation phase, where the artifact (certification maturity model) is evaluated through expert interviews with stakeholders from the field. The validation is structured according to the Unified Theory of Acceptance and Use of Technology (UTAUT), which is an adaptation of the original Technology Acceptance Model (TAM).

Chapter 7 discusses the results, limitations and reflects on potential threats to the validity of this research.

Chapter 8 covers the conclusions of this master's thesis. Section 8.1 lists the novel contributions presented by this research project. Section 8.2 provides answers to the research questions. Section 8.3 presents practical implications for practitioners from the field, academic researchers and provides suggestions for future work.

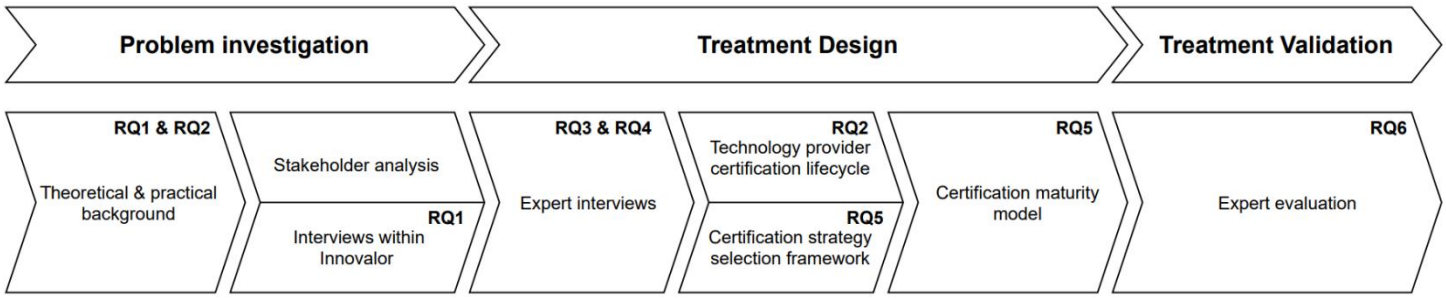

Figure 2: Resarch framework.

2 Background

As mentioned in the introduction chapter, in preparation for this master's thesis, the author of this research conducted a systematic literature review. In order to not self-plagiarize, we take this opportunity to inform the readers that sections 2.2 and 2.3 summarize the literature review findings and incorporate direct body of text from the review. The literature review was done as a Research Topic paper preceding the execution of the master's thesis project. This review revealed commonly reported benefits and challenges of information security certification, as well as commonly adopted security standards and frameworks [3]. Section 2.2 explains the IT certification process. Section 2.3 discusses relevant findings from the literature review and section 2.3 provides an overview of prominent developments within the field of security certification.

2.1 Certification Process

The information security certification process revolves around compliance with developed information security standards. The certification process is built as an infrastructure of trust and operates based on two concepts called *accreditation* and *certification*. Accreditation is "*the action or process of officially recognizing someone as having a particular status or being qualified to perform a particular activity*" (Oxford Dictionary[8]). As discussed in section 1.2, certification is "*the action or process of providing someone or something with an official document attesting to a status or level of achievement"* (Oxford Dictionary[9]). In practice, certification is often seen as assurance by an independent third party that an organization is operating conform certain security standards, whereas accreditation is the recognition of being qualified to grant certification.

However, not all certifications are necessarily given out by third parties. Daskalova and Heldeweg [10] distinguish between the following three types of certification:

- First party (self-certification): Certification where the conformity assessment is performed by a certification subject, also known as self-assessment.
- Second party (associated certification): Certification based upon assessment by an associated party, with an interest in the object, such as by an employer or a branch organization.
- Third party (independent certification): Certification based upon an assessment by an independent party such as an accredited private company or public authority.

Given that Innovalor is primarily involved with information security, the scope of this research is limited to information security certifications and standards. In practice, we almost exclusively see the adoption of third party information security certification, because first and second party certification are often considered insufficient in generating customers' trust. As such, when discussing certification in this research, unless stated otherwise, we implicitly refer to third party certification.

Salminen [11] explains the roles of actors in the accreditation-certification process well, describing it as a hierarchic structure with accreditation agencies being at the top. In the Netherlands, the national accreditation agency is the Raad van Accreditatie (Accreditation Council, hereinafter: RvA [10]). Accreditation agencies are tasked with the responsibility of validating the competence of certification bodies based on accreditation regulation. The certification bodies can grant certifications based on their own audits or audits performed by competent auditing agencies. Competent auditing agencies perform IT audits through their IT auditors [11]. IT auditors examine and evaluate an organization's IT systems by checking whether the organization complies with certain standard(s) based on generic audit controls to identify risks and catch any fraudulent practices. The standards are developed by organizations known as standardization bodies, which do so based on drivers such as regulation, interoperability and trust. We have constructed a high-level overview of the certification process based on the process as described above, depicted in Figure 3 below.

[8] https://www.lexico.com/definition/accreditation
[9] https://www.lexico.com/definition/certification
[10] https://www.rva.nl/

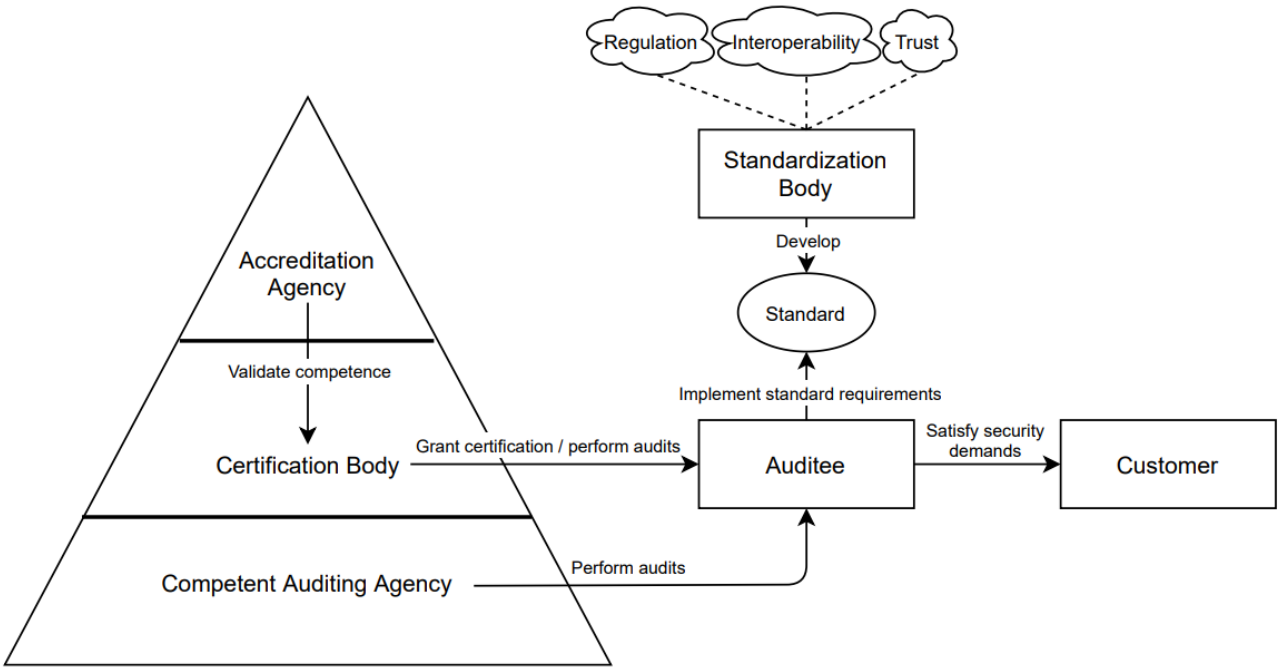

Figure 3: High-level overview of the certification process.

Although only accredited certification bodies have the authority to grant certifications, not every standard is accompanied by matching accreditation. It is still possible to perform audits (conform standards) and provide assurance despite the lack of accreditation, but the value of the assurance then depends on the reputation of the auditing agency.

2.2 Systematic Literature Review (SLR)

This section summarizes the main conclusions of the systematic literature review in order to provide a general theoretical background. Specific findings from the literature review that were deemed relevant to this thesis were incorporated in the results section of this research (discussed in Chapter 4). The literature review investigated four research questions and came to the following conclusions [3]:

RQ 1: *What are the benefits of information security certification according to the literature?*

The most pronounced benefits appear to be effective reduction of risks due to:

- Increased security measures.
- Trust establishment.
- Promotion of organizational security management and governance.

RQ 2: *What are the challenges of information security certification according to the literature?*

The most pronounced challenges appear to be inadequate security assurance due to:

- Genericity of frameworks.
- Increasing complexity of the IT security audit landscape.
- Significant financial costs associated to certification.
- Dependence on individual auditor competence.

RQ 3: *What are the success factors of information technology audits, according to the literature?*

In the context of IT auditing, success factors are defined as factors that, when managed properly, positively affect the outcomes of an IT auditing project. The most prominent success factors come from Merhout and Havelka's [12] IT audit success factor model, which defined the following eight factors:

- Audit process.
- Social IT auditor competence.
- Technical IT auditor competence.
- Audit Team
- Client-controlled organizational factors.
- IT audit-controlled organizational factors.
- Enterprise & organizational environment.
- Target process & system.

RQ 4: *What are commonly adopted security frameworks and standards according to the literature?*

Based on the occurrences within the academic literature, a distinction was made between general information security frameworks, financial sector-specific frameworks, and healthcare sector-specific frameworks. The most adopted frameworks and standards are:

- General information security certification: ISO/IEC 27001, COBIT, ITIL, Common Criteria and the NIST/FISMA risk management framework.
- Financial sector-specific certification: PCI DSS and SOC 2.
- Healthcare sector-specific certification: HIPAA Security Rule (United States) and NEN 7510 (the Netherlands).

There is a significant number of available information security frameworks and standards for products and processes. Some are widely applicable while others are highly sector-specific, with an equally pronounced contrast regarding the differences. Some information security standards appear to be complementary [2],[13] while others share significant amounts of redundancy [4],[14].

It is important to clarify that SOC 2 is not designed specifically for the financial sector, nor is it legally required by regulation in Europe. However, SOC 2 has adopted the role of becoming the financial sector industry standard. In practice, it is practically impossible to operate in the financial sector without acquiring a SOC 2 assurance report from an independent third party.

To conclude, the seemingly contradictory nature of the proclaimed benefits compared to the challenges requires nuance. It is not contradictory evidence, but rather shows the complex nature of the IT auditing process, as well as the complexity of information security, which is not easily captured in a clear auditing framework. As a result, a significant portion of the responsibility within the IT audit process is shifted to the IT auditor. As such, the quality of the IT audit heavily depends on the individual auditor competence.

2.3 Practical Developments

This section discusses practical developments in the field of information security certification and IT auditing.

2.3.1 Component certification

A few initial real-world examples of the concept of component certification can be found in both the ETSI standards designed to comply with the eIDAS regulation and the various ISO standards. Although these operate slightly differently, both of these types of standards support a modular or component-based structure when it comes to certifications (to a certain extent). The core concept of component certification is that a common, often organization-wide security baseline, is extended with a narrower but more specific set of controls in the relevant areas to reduce audit overhead.

2.3.1.1 ETSI standards

The regulation on electronic Identification, Authentication and trust Services (abbreviated as eIDAS regulation), introduced a legal framework for new types of trust services and establishes a scheme for granting qualified status to these new types of trust services. The new services include electronic seals, time stamps, registered delivery services and certificates for website authentication (such as SSL/TLS certificates) [15]. The European Telecommunication Standards Institute (abbreviated as ETSI[11]) have developed a series of European standards for TSPs to comply with the eIDAS regulation.

However, increasing amounts of outsourcing may lead to situations where the scope of a standard can be larger than what is relevant for an auditee. What makes the ETSI standards, catered to TSPs interesting, is the fact that it is one of the first real-world applications of component certification (or sometimes referred to as module certification). ETSI does not allow the auditee to determine the scope or to specify a statement of applicability, but it is possible to exclude areas of the standard that deemed to be not applicable (resulting in different components within one standard). For example, Innovalor has recently acquired an ETSI certification, specifically for the component of identity proofing. This is effectively an initial real-world example of component certification, where only the relevant parts of a standard are implemented and audited.

ETSI defines at least the following list of modules (or components) for organizations within the TSP sector [16],[17]:

- Cryptography.
- Electronic signature verification.
- Identity proofing.
- Signature activation.
- Trustworthy signature creation.

Although ETSI standards in their current state are primarily utilized in the TSP sector (to comply with eIDAS regulation), they may prove to be a suitable candidate as one of the first examples of cross-sector component certification. The need for identity verification occurs in the documentation of multiple sector-specific regulations:

- **Financial sector:** Both the European Anti Money Laundering Directive (4AMLD/5AMLD[12]) and the Dutch *"Wet ter voorkoming van witwassen en financieren terrorisme"* (prevention of money laundering and financing of terrorism act, hereinafter WWFT[13]), explicitly state the need for identity verification. According to the WWFT article 3, organizations in the financial sector must identify and verify a client's identity.
- **Healthcare sector:** Both article 12 in the EGiZ gedragscode (code of conduct for electronic data exchange) [18] and articles 5 and 6 in the *"Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (*supplementary provisions for the processing of personal data in healthcare act*)*[14]*",* state the need for Dutch healthcare providers to identify and authenticate the identity of their customers.
- **Trust services providers (TSPs):** Article 24 from the regulation on electronic identification and trust services for electronic transactions within Europe (eIDAS) specifies that, when issuing a qualified certificate for a trust service, a trust service provider shall verify the identity in accordance with national law for whom the certificate is issued [8].
- **Telecommunications sector:** According to the Richtsnoeren Identificatie en verificatie van persoonsgegevens[15] (*Guidelines for Identification and Verification of Personal Data* in English), telecommunications providers are legally allowed to verify the identity of their customers and ask their customers to show a valid identity document in order to do so.

[11] https://www.etsi.org/about
[12] https://ec.europa.eu/info/law/anti-money-laundering-amld-v-directive-eu-2018-843_en
[13] https://wetten.overheid.nl/BWBR0024282/2020-10-15
[14] https://wetten.overheid.nl/BWBR0023864/2019-07-01
[15] https://wetten.overheid.nl/BWBR0033181/2012-07-12

The draft of ETSI 119 461 on the topic of Electronic Signatures and Infrastructures defines identity proofing as *"the process of proving with the required degree of certainty that a person (the applicant) claiming an identity is the correct person"* [19]. The documentation states that the required degree of certainty is determined by the context, such as the purpose of the identity proofing, the relevant regulatory environment and the acceptable risk. When the applicant is a natural person, the identity proofing process must produce at least one or more of the following:

- A physical or digital identity document.
- An electronic identification (eID) that can be used to authenticate the applicant.
- A digital signature supported by a certificate that identifies the applicant.

It seems reasonable to conclude that the ETSI standard mentioned above can, in theory, be leveraged to comply with all of the abovementioned regulations. This is not to say that ETSI is the be all, end all solution that obviates the need for other certifications, but it shows the potential for highly specific component (or modular) certification with applicability across several sectors.

2.3.1.2 ISO standards

ISO stands for the International Organization for Standardization[16], which is a standardization agency, just like ETSI from the previous subsection. Throughout the years, ISO has developed many international standards, of which the ISO 27001 is the most known. The ISO 27001 standard was published in 2005 and continues to operate as one of the leading security standards for information security management systems (abbreviated as ISMS), particularly in Europe.

As briefly mentioned in section 1.2, the ISO standards are unique in the sense that they tend to complement each other. The ISO 27001 acts as a general organization-wide security baseline which can be extended by other standards such as ISO 27002, ISO 27701 (privacy focus) or ISO 27017 (cloud focus). There are at least a few dozen standards in the 27000 series, but not all of these extend the 27001 and not all of these can be certified for. That being said, it is clear that ISO recognizes that the 27001 standard, on its own, is insufficient in certain scenarios and that the applicability of additional security controls depends on the context an organization. The control scope of the ISO 27001 certification is typically defined in a separate statement of applicability document.

2.3.2 Amazon AWS control framework

Amazon is one of the largest players in the world when it comes to providing cloud hosting as a service, specifically through their Amazon Web Services (abbreviated as AWS). As such, it is not surprising that they employ their own tactics when it comes to security assurance. Amazon constructed what they refer to as the Shared Responsibility Model, which is effectively their own security controls framework. It assigns responsibilities between Amazon and customers and explains what security controls it has in place. Specifically, it distinguishes between three types of security controls:[17]

- Inherited Controls: Controls that a customer inherits from AWS, meaning that they are security controls for which Amazon takes responsibility.
- Shared Controls: Controls for which AWS provides the requirements and the customer implements these within their use.
- Customer Specific Controls: Controls for which the customers are responsible.

Amazon maps its own security control framework onto existing standards to show that they are compliant with the many different security standards. This is done in a single document, where Amazon's controls are accompanied by a reference to the relevant control(s) from other standards, such as ISO 27001, SOC 2 or ETSI. The benefit of such an individualized security framework is that, when Amazon's security controls are changed or a security standard is updated, only one document has to be altered. Moreover, the mapping of the controls to the appropriate certifications is documented in one central location, providing Amazon with a clear overview of all the acquired certifications. It paints the picture of the overlap between certifications and ensures that an organization knows from where a certain security control originates.

[16] https://www.iso.org/home.html
[17] https://aws.amazon.com/compliance/shared-responsibility-model/

The construction of such a framework is a labor-intensive process, because it requires an extensive analysis of all relevant certifications in order to properly map them according to a company's own security controls. However, once constructed, maintenance should be a relatively simple process.

2.3.3 ENSIA single information audit

ENSIA (Eenduidige Normatiek Single Information Audit) is project started by the Dutch government aiming to professionalize the supervisory process of information security at Dutch municipalities. It is based on Dutch information security regulations across various sectors, such as the BIG (Baseline Informatieveiligheid Gemeenten or *Baseline Information Security Municipalities* in English) and BIO (Baseline Informatiebeveiliging Overheid or *Baseline Information Security Government* in English).[18]

Dutch municipalities are required to fill out annual self-evaluation questionnaires in combination with a yearly audit. It is essentially a collection of several sub-auditing frameworks to provide IT auditors with a uniform single auditing framework for governmental agencies, although it shares significant resemblance with the ISO 27001. According to the ENSIA manual, the ENSIA auditor of a municipality takes responsibility and cooperates, where possible, with the external auditor. The auditing efforts can be reduced if the external auditor constructs an auditing report conform the ISAE (International Standard on Assurance Engagements) 3402 type 2/SOC 2 reporting guidelines [20]. In essence, ENSIA can be regarded as an example of a commonly agreed upon national cross-sector standard.

However, using the term ''commonly agreed upon'' can be regarded as misleading in the case of ENSIA, because it was effectively imposed by the government, specifically in the context of municipalities. Thus, by definition, it is not commonly agreed upon. For non-governmental agencies any attempts at achieving a similar type of cross-sector certification would likely require the different regulatory agencies and standardization bodies to communicate in an attempt to come to a commonly agreed upon standard.

[18] https://www.ensia.nl/wat-is-ensia/#!/

3 Research Methodology

This chapter presents the research methodology followed in this research project. Section 3.1 discusses the research method that was adopted as the foundation for establishing our research process. Section 3.2 describes the data collection process, as well as the approach that was followed for the data analysis. Section 3.3 describes how the problem investigation phase is structured. Section 3.4 describes the process for the establishment of the treatment design. Finally, section 3.5 explains how the proposed treatment is validated.

3.1 Method

The research method of choice for this research is the Design Science Research Methodology (DSRM) developed by Wieringa [9], which focuses on the interaction between an artifact and the relevant context, that contributes to solving a problem. It consists of two parts, designing and investigating artifacts in a given context.

Design science distinguishes between two types of research problems: *Design problems* and *knowledge questions*. Design problems require analysis of stakeholder goals to come up with a design that can achieve a real-world change. There is no single best solution as there can be different solutions (designs) for the same problem. The value of a given design depends on the relevant stakeholder goals. Knowledge questions do not call for a real-world change and instead try to answer a knowledge question with the assumption that there is only one correct answer. According to Wieringa, the task of designing consists of three activities: Problem investigation, treatment design and treatment validation [9]. Together, these three form the design cycle, which is a subset of a larger process called the engineering cycle. The engineering cycle is an iterative rational problem-solving process used to structure design science research, depicted in Figure 4.

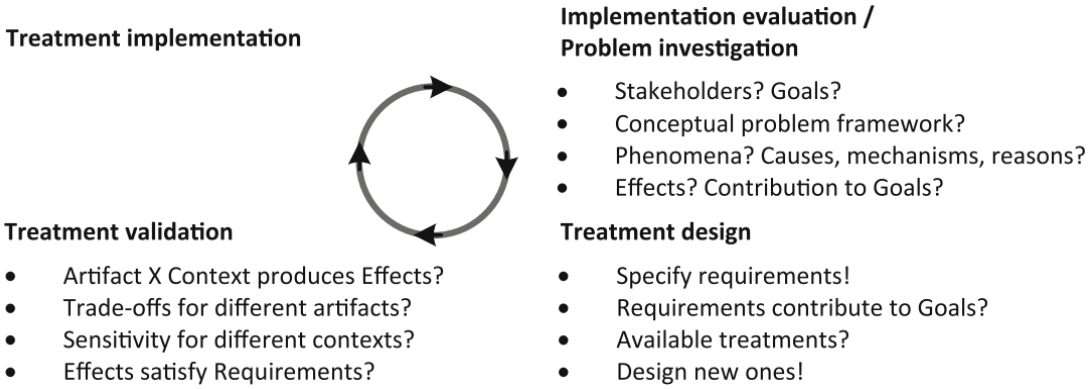

Figure 4: The engineering cycle.

The design cycle encompasses the first three steps of the engineering cycle, which is the problem investigation, treatment design and treatment validation. The engineering cycle also includes the treatment implementation and implementation evaluation. The concept of implementation evaluation is similar to the problem investigation; hence they are grouped together. Given the time constraints, the scope of this research is limited to the design cycle (problem investigation, treatment design and treatment validation).

First, the problem investigation answers the question of what phenomena must be improved and why. In this research, the problem being investigated is: *What are the challenges that technology providers, such as Innovalor, experience when trying to meet their customers' security requirements?* This problem is answered through a combination of a literature review, stakeholder analysis and semi-structured qualitative interviews with experts. The approach for the problem investigation can be found in section 3.3 and the results of the investigation are presented in section 4.1.

The second phase is treatment design. Based on the academic literature and recent developments in the field of security certification, this research first identifies which components from existing treatments are relevant for technology providers looking to be certified. Based on these results, initial candidate strategies are hypothesized, which experts from the field are asked to reflect on. The approach for the treatment design can be found in section 3.4 and the results of the investigation are presented in section 4.2.

The final phase addresses treatment validation, where it is justified whether the treatment contributes to stakeholder goals when implemented in the problem context. In short, the aim of treatment validation is to predict what happens if the treatment gets implemented in the future. To accomplish this, the research method of choice for this research is validation by expert opinion. The treatment is submitted to a panel of experts to determine how it interacts with the problem context and predict and whether it satisfies the user requirements. The treatment validation approach followed in this research can be found in section 3.5 and the results are presented in section 6.

3.2 Data Collection & Analysis

In this thesis, data was collected from two sources. First, a literature review regarding the value of information security certification was conducted in preparation for this research. It identified commonly reported benefits and challenges associated with adopting information security certifications in order to identify the value of certifications. In addition, the review identified commonly adopted standards and summarized eight success factors that contribute to positive outcomes of IT auditing projects.

Secondly, additional data was collected from qualitative semi-structured interviews with experts from the field. Interviews were conducted in both the problem investigation and treatment design phases. The content of the questions and purpose of the interviews was similar, but not identical between each phase. The qualitative research guidelines of King et al. [21] and the qualitative interview guidelines of Roberts [22] were used as methodological sources for designing the interviews in this research project.

The qualitative data collected through these interviews was analyzed by using the coding techniques as per Saldaña, who defines coding in the context of qualitative inquiry as *"most often a word or short phrase that symbolically assigns a summative, salient, essence-capturing, and/or evocative attribute for a portion of language-based or visual data. The data can consist of interview transcripts, participant observation field notes, journals, documents, drawings, artifacts, photographs, video, Internet sites, e-mail correspondence, literature, and so on"* [23]. Finally, the data collection approach as described in this section refers to both the interviews for the problem investigation and the treatment design phases.

3.3 Problem Investigation

The problem investigation exists of two parts: A stakeholder analysis followed by qualitative semi-structured interviews. Each of these parts are elaborated on in their respective sections.

3.3.1 Stakeholder analysis

According to Wieringa [9], a stakeholder of a problem is *"a person, group of persons or institution affected by treating the problem."* The goal of a treatment design is to improve the outcomes of one or more stakeholders, but it is important to consider that a treatment may result in negative outcomes for some stakeholders as well. To aid with understanding stakeholder desires and goals, the relevant stakeholders for this research were identified and classified according to the stakeholder taxonomy developed by Alexander [24]. In accordance with the information security certification process (explained and depicted in Figure 3), the relevant stakeholders are defined in Table 1.

Stakeholder	Relevant role(s)	Classification
Innovalor	Compliance officer, security architect, CEO	Sponsor & functional beneficiary
Auditees	Technology providers (compliance & security)	Functional beneficiary
Customers	Outsourcing organizations (compliance & sales)	Financial beneficiary
Auditing agencies	IT auditors, Certification bodies	Negative stakeholder
Standardization bodies	ISO, NEN, ETSI, ISA, ITU, CENEC	Consultant
Accreditation agencies	Raad van Accreditatie (Accreditation Council)	Consultant
IT security experts	IT security consultants	Consultant
GRC tool suppliers	Cybermanager, Complions, Cerrix, Smile	Consultant

Table 1: Stakeholder analysis.

The sponsor initiates the research and provides the budget for the development of the artifact, hence Innovalor is the sponsor of this research. Functional beneficiaries benefit from the output produced by the artifact. In this research the auditees are the functional beneficiaries as they would benefit the most from choosing the correct information security certification strategy. Although Innovalor is the sponsor of this research, they also function as auditees, which is why they are both sponsor and functional beneficiary. In general, auditees consist of technology providers looking to meet their customer's information security demands. Within these technology providers, the compliance and security departments tend to be primarily involved with information security certification. In the case of Innovalor, the CEO (Chief Executive Officer) is involved as well due to his technical background and experience.

The customers are organizations that outsource part of their processes to technology providers. They are classified as financial beneficiaries, because they do not interact with the artifact directly, yet benefit financially from an improvement in the auditee's certification strategy. Assuming that an appropriate certification strategy results in an improvement in the assurance level, it allows customers to rely on the auditee's certification and eliminates (or at the very least diminishes) the need for customers to perform their own audits. The customers can perform fewer audits or reduce the audit duration, resulting in decreased auditing costs.

Moving on to the auditing agencies, the certification process that was described in section 2.1 and depicted in Figure 3 distinguishes between competent auditing agencies and certification bodies. However, in practice, the line that separates these two entities is often blurred, because an IT auditor may very well be responsible for both conducting the audits and granting the certification. As such, for the sake of simplicity, they are classified as one single stakeholder type under the umbrella term of auditing agencies. It is not beyond any reasonable stretch of the imagination to consider that not all stakeholders involved in the certification process will benefit from a specific strategy. The auditees' interests may not necessarily be aligned with the auditors' interests. For example, an auditee may desire the elimination of (highly) redundant certifications, which would inevitably result in a reduction of the auditor's workload. From a business perspective, a reduction of auditing workload may be desirable for some, but unwanted for others. Some certification strategies might even result in better outcomes for both the auditee and auditor. As such, it is not necessarily one or the other. The main takeaway is that not all involved stakeholders necessarily benefit from the proposed treatment, with IT auditors being more likely to be affected negatively.

The remaining four stakeholders, namely the standardization bodies, accreditation agencies, IT security experts and GRC tool suppliers, are classified as consultants. What these stakeholder types have in common is the fact that they support the development of the artifact, but do not directly interact with the artifact. Standardization bodies are responsible for the creation and maintenance of information security standards, which is why their input can be invaluable for shaping the development of the artifact. They primarily track the developments in the market and develop standards for satisfying the emerging security demands. Accreditation agencies validate the competence of certification bodies based on accreditation regulation and may provide the perspective of a supervisory body. IT security experts work with information security on a daily basis and may offer valuable insights into the best practices of IT security. Finally, GRC tooling suppliers are organizations that develop Governance, Risk & Compliance tooling. These tools aid in the management of information security management systems (ISMS).

3.3.2 Interview Structure for the Problem Investigation Phase

The literature review conducted in preparation for this research revealed a multitude of common challenges associated with information security certification [3]. However, in order to assess the practical problems that Innovalor experiences, qualitative semi-structured interviews were conducted with three employees from the company. These problem investigation interviews serve four purposes:

- To verify the problems that were identified in the problem statement (section 1.3).
- To generate ideas for the construction of certification strategies.
- To compare findings from the literature review (section 2.2) to experiences in practice.
- To receive feedback on the practical developments discussed in section 2.3.

As discussed above in section 3.2, the interview data was analyzed by using the coding techniques as per Saldaña [23] and the questions were designed according to the guidelines of King et al. [21] and Roberts [22].

The interviews consist of just over ten open questions that are available to the readers of this thesis in Appendix A: Problem investigation interview questions. Regarding the interview structure, the interviewees were first asked to explain the necessity of information security certifications and what their specific certification processes look like. The participants were then asked to describe their security certification challenges and reflect on our initial understanding of the problems. The participants' reflections on the initial problem analysis clears up any differences in interpretation or communication and ensures an accurate depiction of the situation.

The remainder of the questions are geared towards exploring existing treatment options. The interviewees may already have considered some strategies of their own, such as the concept of component certification as a means to solve the identified challenges. Moreover, given the multidisciplinary background of the participants, it is not unreasonable to consider the possibility of running into seemingly contradictory opinions among the responses. This could prove to be invaluable when considering the impact of differences in perspective when considering different strategies later on in the research.

3.4 Treatment Design

In this research, treatment design is about designing an artifact that can solve the problems associated with meeting the sector-specific information security requirements, based on the results of the problem investigation. First, available existing treatments were collected based on the literature and the results of the problem investigation interviews. Findings from the existing treatments were incorporated into the construction of initial certification strategies. Additionally, novel strategies were developed based on the problem description, literature review and interview data. Given the fact that the author of this research has insufficient practical knowledge in the field of security certification, qualitative interviews were conducted with stakeholders from the field, who were asked to reflect on the different strategies. The experts commented on the different strategies and identified potential strengths, weaknesses and situational factors.

3.4.1 Interview Structure for the Treatment Design Phase

The aim of the interviews is to combine the participants' area of expertise to determine the most suitable treatment candidate for a given situation. Of particular interest is to see the degree to which the interview responses converge towards a consensus or whether there are notable differences (perhaps even conflicting interests). Moreover, the interviews show the degree to which the challenges that were identified by Innovalor are generalizable and whether they agree on the most suitable treatment candidates. To this end, the treatment design interviews serve three purposes:

- To assess the generalizability of Innovalor's problems across technology providers.
- To evaluate the proposed certification strategies.
- To generate novel ideas for addressing the certification challenges.

As discussed above in section 3.2, the interview data was analyzed by using the coding techniques as per Saldaña [23] and the questions were designed according to the guidelines of King et al. [21] and Roberts [22].

Particular attention was paid to the wording of the interview questions to ensure that the questions align closely with the topic being explored. In addition, all interview participants were assured of complete anonymity to ensure that no harm would befall the research participants and allow them to speak their minds freely. What separates the treatment design interviews from the problem investigation interviews, is that the participants were first presented with the challenges reported by Innovalor regarding information security certification and asked to reflect on these issues. We then proposed different strategies for satisfying security demands whilst alleviating some of the financial and/or continuous auditing burdens, which the participants were asked to reflect on and were given the opportunity to contribute with strategies of their own.

All interviewees were given a similar set of questions. However, different types of stakeholders call for minor adjustments. Therefore, a small set of stakeholder-specific questions were included to utilize the interviewees' specific areas of expertise. The list of interview questions is available to the readers of this thesis in Appendix B: Treatment Design Interview Questions.

Technology providers were asked about their certification strategies and to reflect on the kind of issues they encounter. Standardization agencies were asked about the significant degree of overlap among different sectors, countries and degree of cooperation with other standardization bodies. Lastly, the IT auditors were asked in detail about the differences between the common security standards and the feasibility of the proposed strategies. Just as with the problem investigation, the qualitative data collected through these interviews was analyzed by using the coding techniques as per Saldaña [23].

In contrast to the problem investigation interviews, the treatment design phase calls for a larger sample size. According to Mason [25], the guiding principle for determining the sample size of qualitative interviews is the concept of saturation. Saturation is reached when the collection of new data does not shed any further light on the issue under investigation. According to Charmaz [26], the narrower the scope of the research, the smaller the sample size can be and suggests that 25 participants are adequate for smaller project. In addition, Guest et al. [27] suggested that a sample size of 15 is the smallest acceptable number of respondents. That being said, the literature on qualitative interviews even revealed research done with sample sizes as small as 5 respondents [28].

For the purpose of this research, we take a closer look at recommendations regarding phenomenological studies. Neubauer et al. define phenomenology as "*a form of qualitative research that focuses on the study of an individual's lived experiences within the world"* [29]. This research investigates the challenges surrounding information security certification that Innovalor experiences as a technology provider and assess effective strategies for meeting the security demands. Regarding phenomenological research, Polkinghorne [30] recommended a sample size between 5 - 25 participants, which was further supported in a recent publication by Cresswell and Poth [31].

It appears there is no set-in-stone approach for determining optimal sample size. A reasonable approach depends on numerous factors such as interview structure, participant homogeneity and research scope. As such, we aimed to interview between 5 - 15 participants in line with the phenomenological qualitative interview guidelines. However, the concept of saturation was leading in determining whether the sample size yielded appropriate results for answering the research questions of this thesis. Lower sample sizes ought to be properly justified and demand transparency of the limitations. Moreover, a tactic known as triangulation was employed, which entails crosschecking the data with the help of a multitude of sources by supplementing the interview data with data from both scientific and grey literature.

In the pursuit of maximizing saturation given the time constraints, a slightly higher number of participants were interviewed for the treatment design phase, resulting in a total sample size of 18 participants. It is worth nothing that some of the interviewed experts had working experience in more than one role, which classifies them under multiple stakeholder types (and thus the total number of participants per role exceeds 18). The breakdown of stakeholder types is characterized as follows:

- IT auditors: 9 participants.
- Technology Providers: 6 participants.
- Standardization agency: 4 participants.
- IT security experts: 4 participants.
- Accreditation agency: 1 participant.
- GRC Tool supplier: 1 participant.

3.5 Treatment Validation

According to Wieringa, the goal of treatment validation is to justify that the treatment contributes to stakeholder goals when implemented in the problem context [9]. There are multiple ways to do so according to Wieringa's methodological source. However, in this thesis, we opt to validate the designed artifact by means of expert opinions. The reason for choosing this approach is because of its suitability to our research context and the peculiar organizational context created due to the Covid 19 restrictions. The proposed artifact is submitted to a panel of experts, who are asked to assess what effects they think the proposed solution would have if it would be implemented in practice. The validation model of choice for this thesis is based on the Technology Acceptance Model (hereinafter TAM) developed by Davis in 1989 [32]. In short, TAM utilizes *perceived ease of use* and *perceived usefulness* to predict the success of information technology.

Despite its introduction more than 30 years ago, TAM remains to be the most preferred model for predicting user acceptance of information technology. However, since its original release in 1989, many researchers have continued to expand upon the original model. One of the more recent improvements of TAM is the Unified Theory of Acceptance and Use of Technology (hereinafter UTAUT), developed by Venkatesh et al. [33] in 2003. UTAUT has been proven to be useful in assessing the likelihood of success for new technology introductions and helps managers with understanding the drivers of acceptance. As such, we chose to validate as per the UTAUT model depicted in Figure 5.

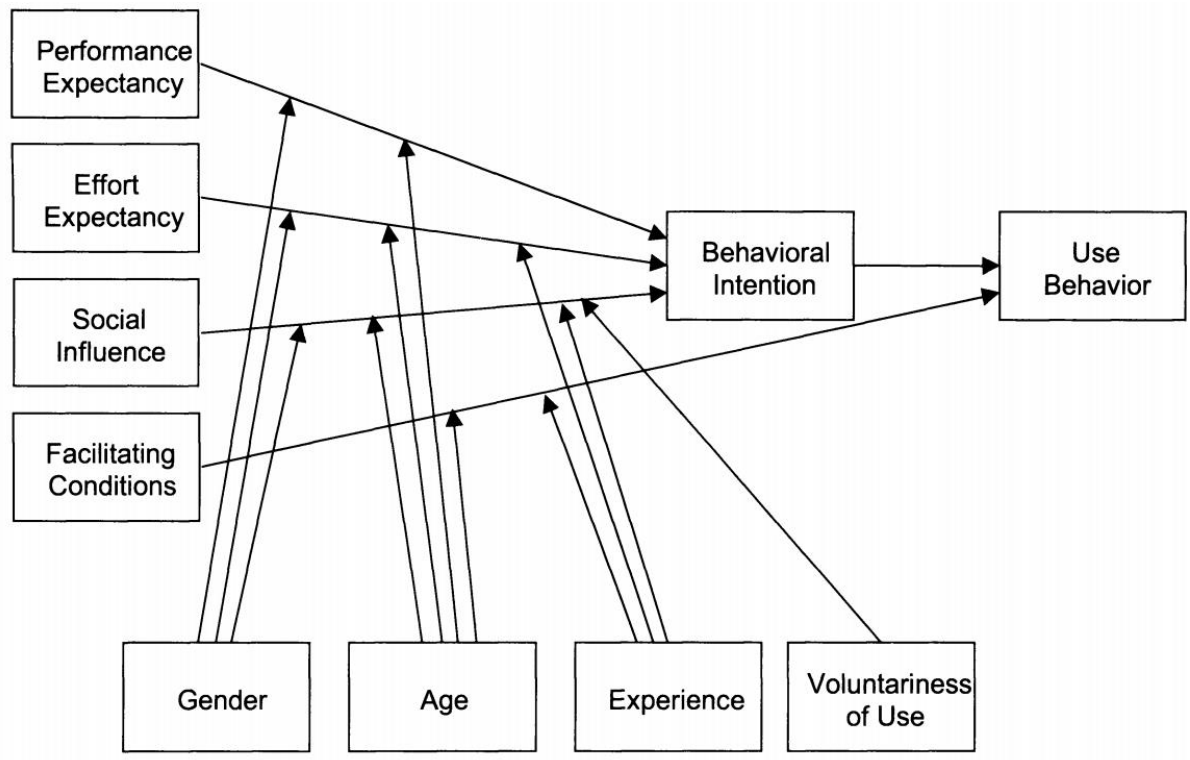

Figure 5: UTAUT by Venkatesh et al. [33]

In 2005, Spil released a set of UTAUT questionnaire items that can be used for the validation or evaluation of information technology [34]. This set of predefined questionnaire items was adapted to the validation of the proposed artifact in this thesis. Four experts within Innovalor and five experts outside of Innovalor were interviewed about the applicability and usability of the proposed artifact in the context of technology providers. The full set of adapted interview questions is available to the readers of this thesis in Appendix C: Treatment Validation Questionnaire (UTAUT)**.**

4 Results

This chapter presents the results of this research and comprises several sub-sections. Section 4.1 covers the results of the problem investigation interviews conducted within Innovalor, in addition to analyzing how these practical findings relate to the theoretical findings from the systematic literature review. Section 4.2 analyzes the treatment design interviews, formulates certification strategies and puts these into perspective by placing them in a single strategy selection framework. This framework shows the relevant certification strategies based on the context in which a technology provider operates in, given the business driver to acquire as many customers as possible across a variety of sectors and industries.

4.1 Problem Investigation

This section analyzes the results from the problem investigation phase. We first summarize the relevant findings from the interviews followed by an analysis of these findings in comparison to the literature discussed in the background chapter (see chapter 2).

4.1.1 Interview results

Three interviews were conducted with employees of various backgrounds, namely the security architect, compliance officer and CEO of Innovalor. The full set of interview questions is available to the readers of this thesis in Appendix A: Problem investigation interview questions. Most employees within the company have little to no interaction with certifications and managing IT audits, hence only these three employees could speak on the topic. The responses were relatively consistent despite the difference in backgrounds. Unless stated otherwise, the interview findings were not conflicting among the participants. The results of the problem investigation have been summarized in a mind map, depicted in Figure 6 below. Therein, we present three categories of concepts: Reasons (the green area), strategies (the blue area) and challenges (the red area). The remainder of this section goes into detail on these three individual aspects from the mind map. This sub-section (4.1.1) merely summarizes and reports the findings that were brought up during the interviews. The analysis of these results can be found in the next sub-section (4.1.2). To improve readability, we note that in our description of the results in sub-section 4.1.2, the concepts in the circles in the mind map are given in *italic.*

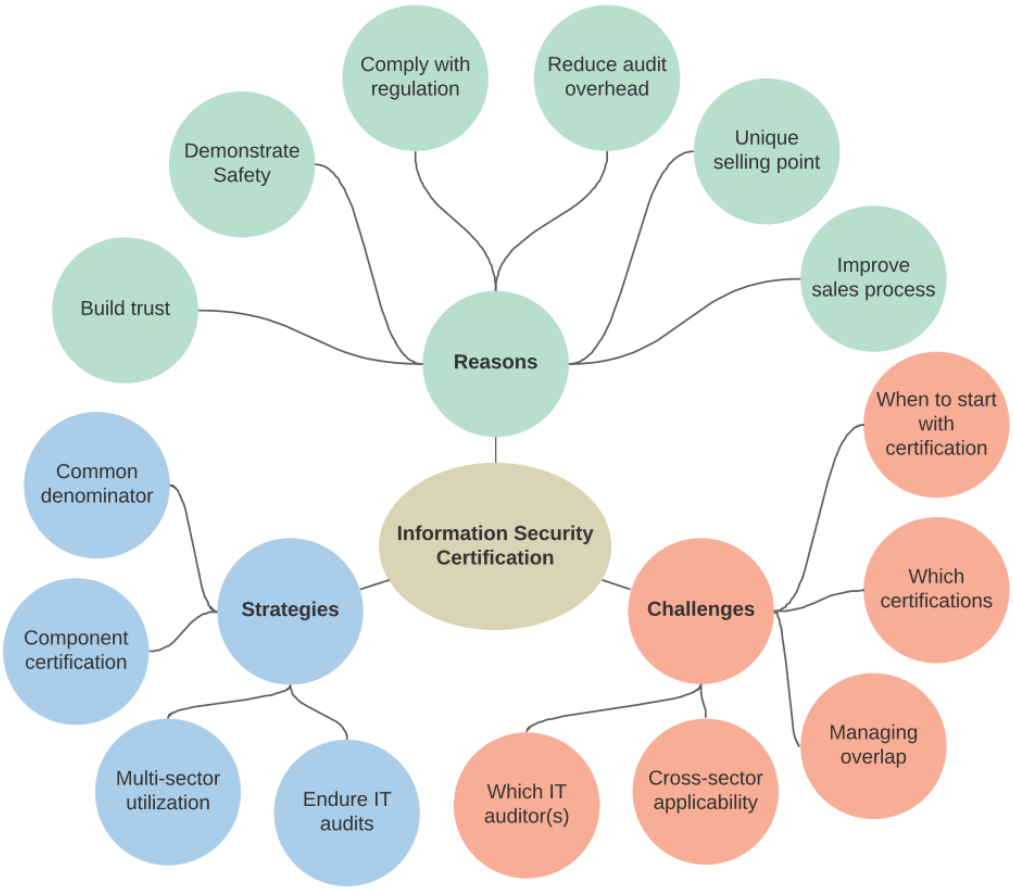

Figure 6: Problem investigation mind map.

Reasons for adopting certification
The customer demands are leading in the decision to adopt a certain certification. Customers desire some form of demonstrable assurance that Innovalor operates securely and is a *trustworthy partner*. Appropriate certification accomplishes this, because compliance to security standards shows that an organization has correctly implemented a set of best practices regarding information security, which *demonstrates safety* based on assurance form an independent third party. As such, certifications are capable of generating trust from the customers.

Some customers prefer (but do not demand) certification, because of the sensitive nature of working with personal data and the fact that many customers have little experience with outsourcing data processing to an external organization. Other customers, however, outright require a technology provider to be certified for certain certifications in order to *comply with sector-specific regulation*. Whenever certification is imposed by regulation on one of Innovalor's customers, these certification demands are also passed on to Innovalor. For example, Innovalor works with TSPs who must obtain an ETSI certification from an accredited auditor to comply with eIDAS regulation. As a result, Innovalor obtained an ETSI (module) certification to appeal to customers who only work with certified partners.

When certification is preferred but not required, customers will often agree to a partnership on the condition that they can audit the technology provider themselves. This is done by having the customer's own auditors conduct their own audits at the technology provider to assess whether the security is conform the customers' own standards. Organizations may get away with not having the desired certification (particularly with smaller customers), but in turn accept having to endure audits from the customers. However, too many annual customer audits will inevitably foster an environment with significant audit overhead. As such, the participants mentioned that certifications are an effective means for *reducing the audit overhead* that comes with having multiple customers.

Moreover, information security certifications contribute to the company by utilizing them as a *unique selling point*. Interview participants emphasized that, even if certifications would not be mandatory, they would nonetheless desire an independent third party to assess the organization's security and provide valuable feedback. The participants expressed an intrinsic motivation for wanting to be secure and went on to explain how certifications benefit Innovalor as a unique selling point. Regardless of whether or certification is required, they are marketable and attract customers. Acquisition of appropriate certifications distinguishes oneself from competitors and attracts customers that are willing to pay a premium for higher quality.

Finally, all participants agreed that certifications *improve the sales process*. They enable quick and easy demonstrable compliance without having to open up sensitive areas of the company to potential customers. Certifications provide Innovalor with the opportunity to grant customers access to official audit reports without having to be transparent with other sensitive aspects of the organization. In addition, convincing the compliance and sales departments of potential customers that Innovalor's existing certifications already suffice to address the customers' security concerns remains difficult in practice.

To summarize, the following reasons for adoption were reported:

- To build trust.
- To demonstrate safety with proper security measures and documentation.
- To comply with sector-specific regulation.
- To reduce the auditing overhead and associated costs in order to promote scalability.
- To stand out from competitors by utilizing certification as a unique selling point.
- To improve the sales process by making it easier to demonstrate compliance to customers.

Certification challenges
Some of the challenges were already mentioned in the problem statement (see section 1.3), but were confirmed by the participants during the interviews.

First is the topic of *deciding if and when to start with certifications*. Participants reported that the decision to adopt certification is not straightforward. They are expensive investments and require an appropriate degree of documentation from the auditee's side. When financial resources are limited and the number of customers are low, there may be little to no benefit in acquiring certifications. Moreover, not all customers care for information security certifications. Larger institutions, such as banks, only work with organizations that are certified, but SMEs may not see any noticeable benefit. These SMEs view certifications as drivers of costs without an increase in the quality of the product or service. This concept is easily explained by comparing the expected auditing overhead costs to the certification acquisition costs. Note: These numbers are rough estimates taken from the problem investigation interviews:

- Average costs of enduring audit overhead for the technology provider → €6.000:
  - €1.000 per employee per day.
  - 2 employees.
  - 3 days for a full audit.
- Average cost of a single certification → €25.000.

According to the compliance officer of Innovalor, the facilitation of audits typically takes three days and occupies two employees full-time. As such, the average costs of enduring audit overhead come down to roughly €1.000 * 2 employees * 3 days = €6.000 per customer. Auditing overhead scales linearly with the number of customers, resulting in the following situation (see Table 2 below).

Number of customers	**1**	**2**	**3**	**4**	**5**
Costs	€6.000	€12.000	€18.000	€24.000	€30.000
Costs of certification	€25.000	€25.000	€25.000	€25.000	€25.000

Table 2: Audit overhead costs.

According to the situation as outlined in Table 2, it becomes attractive (for Innovalor) to adopt certification when at least five customers are likely to perform their own audits on a technology provider. It is important to keep in mind that one should not blindly look at the total number of customers, just the ones that would conduct their own audits in the absence of certification. Of course, these audits also occupy resources from the customer's side, which are not visible on the surface from the perspective of a technology provider. As such, one could make the case that the true cost reduction from acquiring certification is even greater, because it reduces the time to audit or flat-out eliminates the need for customers to conduct their own audits altogether.

The challenge described in the previous paragraph leads to the dilemma *of choosing which certifications to pursue* in order to serve as many customers as possible. The participants expressed the desire from the perspective of Innovalor to proactively acquire certification, rather than to wait until a customer expresses an expectation for a certain certification. Choosing the appropriate certification(s) ought not to be taken lightly, given the significant financial and administrative burdens associated with obtaining assurance from an independent third party. Some certifications are only utilized in a specific sector of a given country, whereas others are adopted across a wide range of industries and countries.

Moreover, the participants elaborated on the problematic nature of *managing overlap among acquired certifications*. They stated that no security standard is identical, but many share significant amounts of overlap. Overlap is problematic, because it effectively means that an organization is charged several times for the assurance of identical (or relatively similar) security controls. Ideally, Innovalor would opt for certifications that complement each other, but with sector-specific certifications, this is often not possible. Redundant audits require resources that could have been better spent elsewhere.

As such, the participants struggled with the challenge of *leveraging a given certification across multiple sectors*. Conveying to customers that the existing security measures and certifications already provide a satisfactory level of assurance is no simple task. In theory, it is certainly possible to map one's security controls onto another standard, in addition to publishing the official audit reports. However, from practical experience, the participants reported that these measures are often insufficient at providing a satisfactory level of assurance and generating sufficient customer trust.

Lastly, the IT auditing field is interesting due to its diverse supply of information security standards. However, this diversity further complicates the decision of choosing *which auditor(s)* to work with. Although the process of IT auditing is fairly standardized, and all auditors adhere to the same auditor guidelines, notable differences among competent auditing agencies persist. Different agencies may specialize in different standards, employ different rates, adhere to different levels of strictness and even differ in terms of auditing style. Innovalor opted for an auditing agency that is capable of conducting what they refer to as team audits, meaning that different standards are audited in parallel with a team of auditors who are accredited for different areas.

To summarize, the following certification challenges were reported:

- Deciding if and when to start with certifications.
- Choosing which certifications to acquire.
- Managing overlap among certifications.
- How to utilize the same certification(s) in multiple sectors.
- Choosing the appropriate auditing partner.

Potential strategies
The following ideas were presented during the interviews as potential candidates for dealing with the challenges mentioned above.

First, it is possible to accept audit overhead and *endure being audited* by expanding the compliance department. However, none of the participants thought this was a reasonable solution, given the immense number of required financial resources, time commitment and scalability concerns. Of course, without any certifications at all, customers that require certification for the sake of compliance with sector-specific regulation will be lost. These customers are often larger, more powerful corporations such as financial institutions.

Second, the participants expressed an interest in the feasibility of *utilizing already acquired (often sector-specific) certification across multiple sectors*. This could potentially be achieved by mapping the acquired certifications onto the customers' desired certification. It would require competent compliance officers from both parties in order to convince the customers that the technology provider (Innovalor) is already compliant with their security demands. The idea of this is that the degree of overlap is mitigated by utilizing certifications which already address (the majority) of the desired security concerns.

Utilizing certification across different sectors ties into the concept of *component (or modular) certification*. All participants expressed an interest in the concept of component certification, defined as a general organization-wide security baseline supplemented by specific in-depth product certifications. Component certification could effectively shift the focus from certification based on sector-specific regulation to certification based on competence. In the case of Innovalor, competence would refer to the concept of identity verification and authentication, which is the sub-process for which they are responsible. Ideally, this component would have to be accepted by most (if not all) sectors, because a modular approach can only succeed if it is widely recognized. Despite the unanimous interest in the concept of modular certification, not all participants deemed it a feasible strategy. Participants expressed skepticism regarding the potential limitations due to sector-specific regulations and the willingness of auditors to trust each other's work. In addition, they were skeptical about the risk of standardization bodies to accept other standards and adopt a ''not invented here'' attitude.

That being said, the participants did mention their recently acquired ETSI component certification for identity proofing as an initial pilot to investigate the value of a modular approach. Given the financial sector's preference for SOC 2 reports, the participants also expressed curiosity in the feasibility and efficacy of scoping a SOC 2 assurance report such that it only covers areas that have not already been covered by prior certifications.

The final concept that was brought up in the interviews is the *common denominator* strategy, which involves the construction of an individualized control framework. This concept borrows from Amazon's AWS, where the technology provider constructs its own information security framework and maps its controls to the controls from existing information security standards. If desirable, the controls that frequently appear in multiple industries could then be grouped under some sort of common denominator and certified under one broadly scoped organization-wide certification or assurance report (such as

SOC 2). In essence, this would result in a scenario which one could call “audit once, comply with many”. Two out of the three interview participants expressed the most interest in an individualized control framework, whereas one participant showed most interest in a modular approach.

To summarize, the following ideas for strategies were reported:

- Enduring IT audits by expanding the compliance department.
- Utilizing sector-specific certification across different industries.
- Component certification, such as the ETSI identity proofing certification or a supplementary SOC 2 report on top of existing certifications.
- Common denominator approach (audit once, comply many) through a broad and in-depth SOC 2 report as a potential candidate for obviating the need for some of the existing overlapping certifications.

4.1.2 Comparing the Findings from the Interviews to those from the SLR

This section analyzes the reported findings from the interviews and relates them to the findings from systematic literature review conducted in preparation for this thesis, of which the findings are discussed in section 2.2. The result is a high-level comparison between the theoretical findings from the literature and Innovalor’s practical experiences as practitioners from the field.

In order to put the interview findings in perspective, Innovalor’s perspective regarding the many sector-specific certifications and their overlap was visualized in Figure 7, which is merely a schematic overview based on the interviews. An accurate depiction of the degree of overlap among different information security standards would require extensive mapping and analysis of each standard’s underlying security controls, which is too complex for the scope of this research. Based on the problem investigation interviews, we have constructed our own schematic comparison of several information security standards (depicted in Figure 7 below), which illustrates how these compare to each other as a simplification of the real-world scenario. However, it risks eliminating key factors in an attempt to provide a high-level overview. Future research is required to provide more accurate conclusions regarding the degree of overlap and complementary value of specific information security standards, but this is beyond the scope of this research.

Assurance is plotted on the vertical axis and scope is plotted on the horizontal axis. In the introduction chapter, we explained that IT audits are centered around the three concepts of evaluating whether control measures are designed and documented properly, whether they are implemented, and whether they are working effectively (in Dutch this is the concept of opzet, bestaan en werking). These concepts, listed in order from least assurance to most assurance, describe the extent to which a security measure is evaluated. However, the control measure itself can vary regarding level of detail. In Figure 7, both aspects were summarized as assurance, inevitably losing some degree of nuance between these two distinct aspects. As such, a higher assurance level in Figure 7 means that the security measures are more detailed and/or is evaluated in more detail. The scope on the horizontal axis has also been simplified. Some of the most common categories of security controls were incorporated. Although one could expand the scope with numerous additional control classifications, we argue that the controls displayed on the horizontal axis provide a reasonable representation of real-world circumstances and that additional controls would unnecessarily increase complexity of the graph without adding value for comparing the overlap at a high level.

It is important to consider that SOC 2, NEN 7510 and ISO 27001 are organization-wide standards for information management systems. These certifications permit auditees to determine the scope and relevant controls themselves. NEN 7510 is similar to ISO 27001 in the sense that it is effectively a healthcare sector-specific extension of the ISO 27001 with a focus on privacy. SOC 2 is relatively different from the former two, given that it is an assurance report and not a certification. Due to the difference between SOC 2 and ISO 27001, and the variable scope, it is difficult to provide a general comparison. One organization’s scope may not overlap whatsoever with the scope of another organization, despite being certified for the same standard. In general, SOC 2 provides more specific security controls, raising the average assurance level. The remaining standards are all product certifications with relatively fixed scopes.

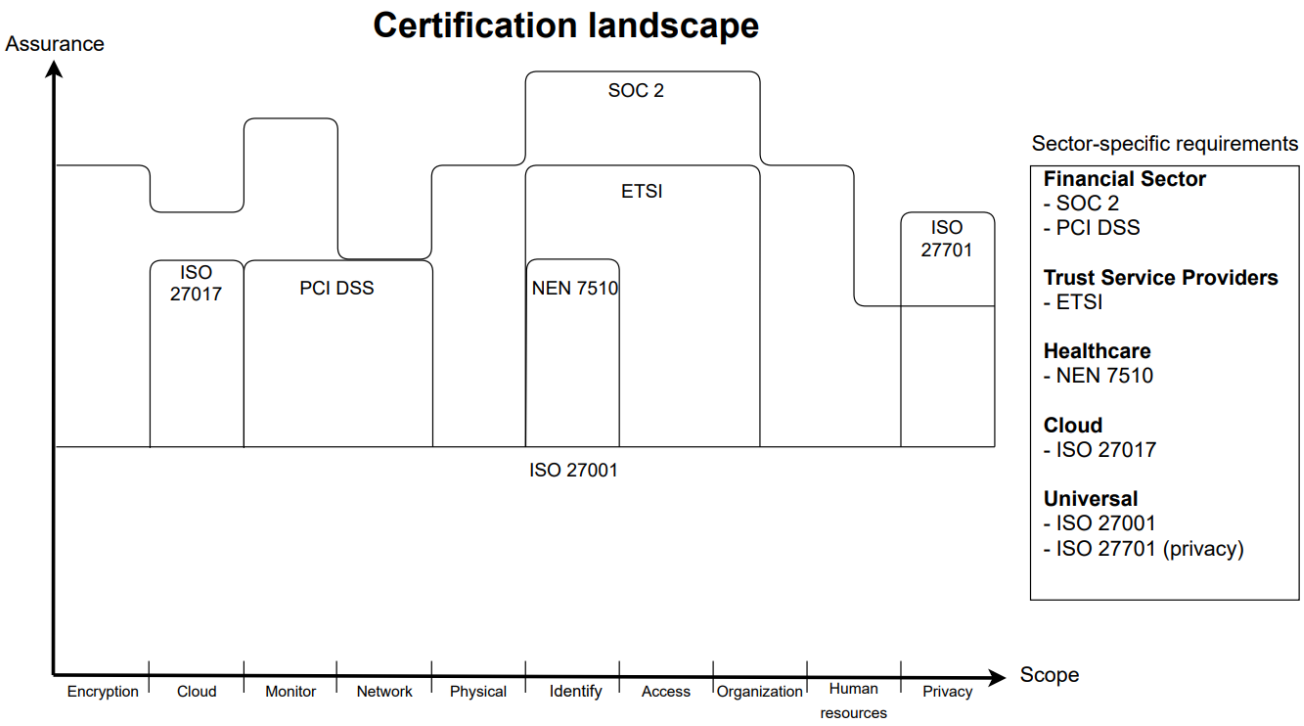

Figure 7: High-level comparison between certifications.

The main takeaway from Figure 7 is that, from Innovalor's perspective, there appears to be a certification jungle with significant overlap among the majority of the standards. Clearly, every standard is different at least to some extent, but it nonetheless raises the question whether the standardization agencies responsible for the development and maintenance of these standards are reinventing the wheel and if so, why that is the case. These concerns were incorporated into the treatment design phase, where stakeholders from the standardization bodies were asked whether they cooperated with other standardization organizations and why that is or is not the case.

When comparing the results of the interviews to the results from the literature review [3], a number of pronounced similarities differences and stand out, which are described below.

The reasons for adopting certifications reflect the findings shown in the literature review. However, a slight disparity persists concerning the financial benefits. While the literature review did report financial benefits, the reported benefits primarily related to future cost reductions, stating *"although research on tangible benefits is limited, there appears to be a potential for financial benefits, primarily in the form of future cost reduction"* [3]. From the interviews, Innovalor put forward the notion that appropriate certification acts as a unique selling point in order to outcompete other technology providers and lead to higher revenue. Effectively, this is the opposite of cost reduction, as it appears to be an investment into the quality of a product/service, raising the costs in order to generate additional revenue.

Regarding the challenges, the findings from the literature differ from the ones reported by the participants. The reported challenges from the interviews primarily relate to resource management. The cost-prohibitive nature of certification proves challenging for organizations with limited capital, because there is pressure on selecting certification(s) that will attract enough customers. As such, cross-sector applicability is one of the most pressing matters for Innovalor. In the literature review, we did mention the cost-prohibitive nature of certifications, but the most pronounced challenges appeared to be inadequate security assurance due to the complexity of the auditing process. In the literature review, we argued that the complexity of IT auditing was multifactorial in nature and described it as "*genericity of large frameworks, a lack of standardized methodology and limited IT audit guidance appear to result in higher audit complexity and a dependence on individual IT auditor competence"* [3].

The discrepancy between financial concerns and security concerns mentioned in the previous paragraph requires nuance. The problem investigation interviews revealed an important aspect of Innovalor's company culture. All participants spoke extensively about the importance of appropriate information security measures, regardless of the certifications for which they are certified. It is our understanding that the participants are confident in their ability to deliver an appropriate level of security regardless of certification, thus making them less reliant on the security assurance aspect of certifications.

Finally, we analyzed seventeen technology providers that are specialized in the field of digital identities (digital signatures, identity verification and access management) in a wider context regarding the adoption of information security certification. Only technology providers operating within Europe were included to ensure a sufficient degree of subject homogeneity and comparability (see Table 3). We analyzed these technology providers by assessing which certifications, standards or regulations they are certified for or compliant with. The color codes of the cells are used to distinguish between these three types of compliance. A green cell shows that an organization has a valid certification. A yellow cell shows that an organization is compliant with, but not certified for a given standard. An orange cell shows that an organization is compliant with regulation and indicates an absence of a standard for that regulation. The results of this comparative analysis are summarized in Table 3 below, which is an original contribution of this research project.

Besides the widespread adoption of ISO 27001, the certification adoption landscape appears complex. It remains difficult to distinguish any apparent pattern in the adoption of information security standard, which emphasizes the current fragmented nature. Moreover, the data from Table 3 seemingly indicates that organizations are struggling to select the right certification strategy.

Organization/ Certification	ISO 27001	ISO 9001	ISO 30107-3	SOC 2	eIDAS (EN 319-401)	PCI DSS	ETSI	Common Criteria	NEN 7510
Mitek	✓			✓					
Veriff				✓ type 2					
Jumio	✓					✓			
Onfido	✓			✓ type 2					
iProov	✓		✓		✓				
FourthLine									
Acuant	✓			✓ type 2		✓			
Evidos	✓			✓	✓				
IDNow					✓		✓		
BioID			✓						
Idemia			✓					✓ EAL 3+	
Thales DIS		✓						✓ EAL 5+	
Regula	✓	✓							
Keesing	✓	✓							
BPI Services	✓	✓							✓
AMP Logistics	✓	✓					✓		
Onegini	✓			✓ type 2					

Type of Certification	Cell color
Certified	
Compliant with standard	
Compliant with regulation	

Table 3: Technology provider certification adoption.

4.2 Treatment Design

The treatment design phase is divided into several sub-sections. Section 4.2.1 depicts the current scenario through a technology provider certification lifecycle. Section 4.2.2 introduces five certification strategies based on the literature, problem analysis and treatment design interviews. Section 4.2.3 introduces four additional general optimization practices that emerged from the interviews, which can be utilized in combination with the certification strategies from the previous section. Lastly, section 4.2.4 puts the five strategies and four optimization practices into one comprehensive framework by mapping them onto the technology provider certification lifestyle that is introduced in section 4.2.1.

4.2.1 Technology provider certification lifecycle

Both the interviews conducted for the problem investigation, as well as those done for the treatment design revealed significant challenges of the current certification process. Regardless of background, interview participants unanimously recognized and acknowledged the challenges reported in 4.1.1. As a first part of the contribution of this thesis, we have constructed a model, based on our interpretation of the literature and interviews, which depicts the current information security certification lifecycle for technology providers down below in Figure 8 and it forms one of the contributions of this thesis.

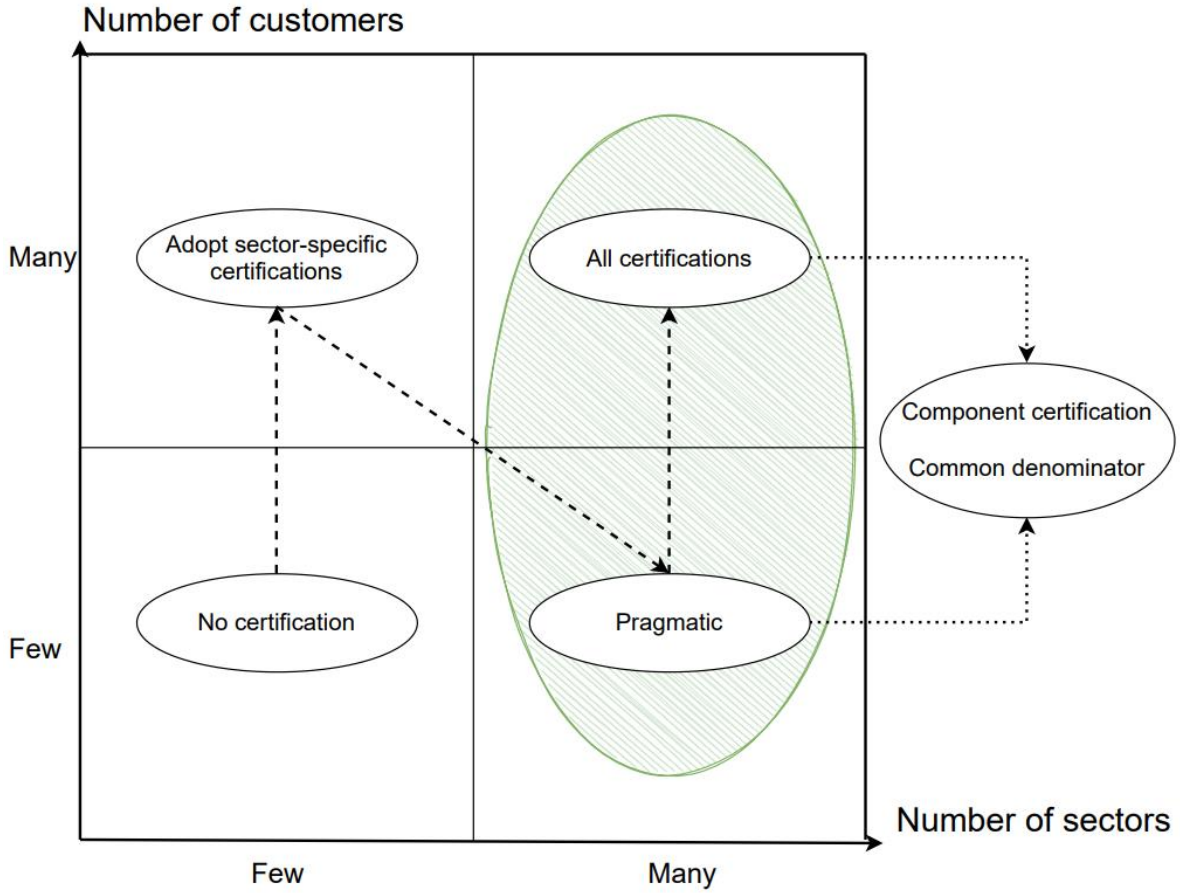

Figure 8: Technology provider certification lifecycle.

The model distinguishes between *four scenarios* based on a combination of the *number of sectors* and the *number of customers*, displayed as a matrix consisting of four quadrants. This model provides a general representation of the different stages of the certification lifecycle for technology providers. The *horizontal axis* displays the number of sectors in which a technology provider can operate, while the *vertical axis* displays the number of acquired customers of a technology provider. A technology provider can operate in either few or many sectors at a given time and a technology provider can have either few or many customers at a given time. What constitutes as few or many depends on the organization, hence why we opted not to use absolute numbers. However, the outcome of Table 2 (see section 4.1.1 regarding the problem investigation interviews) is indicative for the order of magnitude in terms of customers.

Four combinations can be made from the number of sectors and number of customers, resulting in a four-quadrant matrix. The oval shapes inside each of these four scenarios (quadrants) represent our understanding of the commonly adopted certification strategies in the current industry based on the situation in which a technology provider is located. The highlighted green zone represents an area in which both scenarios are viable candidates for the utilization of *component certification* and/or the concept of utilizing a *common denominator* (see the rightmost oval in Figure 8). Lastly, we argue that most technology providers follow a general route, which we call the certification lifecycle, through each of the four scenarios, denoted by the dotted route in Figure 8. The four distinct scenarios are briefly summarized as follows:

- **Few sectors, few customers:** The scenario for startups with limited resources that have not yet been able to generate many customers.
- **Few sectors, many customers:** The scenario for niche SMEs that have grown out of the startup phase by generating more customers, but are still restricted to operating in a small number of sectors.
- **Many sectors, few customers:** The scenario for SMEs that are expanding and branching out into new sectors, exposing themselves to sector-specific certification entry-barriers or significant audit overhead.
- **Many sectors, many customers:** The scenario for larger organizations that have expanded their services across sectors and accumulated a relatively large pool of customers, exposing themselves to higher levels of complexity regarding the management of certifications.

The remainder of this section elaborates on each of the scenarios, as well as the lifecycle route depicted in Figure 8.

Few sectors, few customers: No certification
This scenario is characterized primarily by startups who have little need for certification and/or simply lack the financial resources to acquire them. Every organization starts out with less than a handful of customers in most likely just a single sector, hence the lack of financial resources. Moreover, startups are likely to work with smaller institutions as customers who are not obliged to comply with certification imposed by regulation.

Few sectors, many customers: Adopt sector-specific certification
This scenario is characterized by SMEs that have enough audit overhead to justify acquisition of sector-specific certification(s). Given the fact that they are SMEs, most organizations who fall in this section have little to no record of accomplishment to rely on, which increases the demand for information security certification.

Many sectors, few customers: Pragmatic
This is the most problematic scenario, severely inhibiting innovation of SMEs looking to grow due to certification entry barriers. This scenario appears unsustainable for most SMEs as the current fragmented nature of certification imposes significant compliance burdens on organizations looking to expand their area of operations. Organizations in this scenario are often unable to cope with the certification demands and forced to adopt only the most crucial ones instead. Essentially, it is an unfavorable intermediary phase that technology providers have to endure as well as they can by growing in terms of their certifications.

Many sectors, many customers: All certifications
Although less problematic than the previous scenario, this scenario is attractive from a business perspective, but nonetheless sub-optimal and characterized by complexity, because of the emergence of what we would refer to as a certification jungle due to overlap among sector-specific certifications across an abundance of sectors. As such, this scenario leaves the most room for optimization.

4.2.1.1 Certification lifecycle
In theory, no organization is constrained to following the route outlined in Figure 8. That being said, the technology providers that participated in this research confirmed that these types of organizations generally follow the certification lifecycle as portrayed above. Startups start out in the bottom left quarter, often in a single sector with few customers. As such, there is little to no need for certification and even if there is a need, the financial resources are insufficient to allow for the acquisition of rather expensive certification from an independent third party.

Once a technology provider starts expanding its customer base within a given sector, the financial resources no longer inhibit the acquisition of certification while the demand for appropriate certification simultaneously grows. Additionally, the auditing overhead increases in proportion to the number of customers. This essentially results in a transition from the bottom left quarter (few sectors, few customers) into the top left quarter (few sectors, many customers). Given the homogeneity of the customers, technology providers are steered into the acquisition of relevant sector-specific certifications, reducing the audit overhead and generating trust. In Table 2 of section 4.1.1, we showed how the increase in customers changes the cost-to-benefit ratio, justifying the acquisition of certifications.

Most technology providers possess expertise in highly specialized areas (such as identity proofing or document verification in the case of Innovalor), often only relevant for a certain niche of customers within a given sector. However, these areas of expertise tend to concern generic sub-processes that are not confined to the boundaries of any given one sector. As such, it is nearly inevitable that most organizations eventually expand their services to additional sectors, which introduces significant certification burdens. This transition effectively moves a technology provider to the bottom right quarter (many sectors, few customers). This is problematic, because it causes an imbalance between the number of relevant certifications and the number of customers. As such, it is often unsustainable to simply adopt the additional (sometimes nearly identical) relevant sector-specific certifications. At this point, the significant overlap among certifications makes it so that additional certification is unlikely to result in a superior level of assurance. As such, this scenario imposes significant entry barriers and inhibits innovation of SMEs that would otherwise be able to advance the industry.

If a technology provider manages to overcome the compliance jungle, it eventually ends up transitioning into the top right quarter (many sectors, many customers). Although less problematic in nature (and from a business perspective the most attractive situation in terms of financial revenues), this scenario is nonetheless characterized by inefficiency and complexity in terms of certifications and corresponding audit overhead. At this point, the number of customers justifies the acquisition of additional certifications. However, it becomes increasingly complex to maintain proper oversight. Managing certifications becomes a daunting and time-consuming task that demands careful consideration and an intelligent approach to prevent losing important certifications and to ensure that no certification is unnecessarily extended. Due to its complexity, this scenario allows the most room for optimization.

The main takeaway from the lifecycle portrayed in Figure 8 is that certification needs are situational, meaning that the context in which a given technology provider operates plays a crucial part in the selection of an appropriate certification strategy. For instance, given the certification overhead of the top right quarter, a technology provider could very well decide to stay in the top left quarter, because of the affiliation is has with a certain sector.

In the next sub-sections – 4.2.2 and 4.2.3, we will present five certification strategies (4.2.2) and four general optimization practices (4.2.3). These resulted from two analytical processes in this research, namely (i) the analysis of the problem investigation and (ii) the analysis of the treatment design interviews. In sub-section 4.2.2., five strategies for information security certification were constructed based on the problem investigation results and the practical developments discussed in section 2.3. After this, in sub-section 4.2.3, we report four general optimization practices that came out of the treatment design interviews, which can be applied on top of the five strategies. In both sections 4.2.2 and 4.2.3, we explain the need for these respective strategies and optimization practices. In section 4.2.4, we put all the strategies in context by providing a comparative analysis and combine them together into one conclusive framework.

4.2.2 Certification Strategies Constructed Based on the Problem Investigation

This sub-section introduces five strategies that were constructed based on the problem investigation in detail. We define the following five strategies:

- **No certification by an independent third party (section 4.2.2.1):** Refrain from acquiring certification by an independent third party and accept additional audit overhead.
- **Sector-specific certification (section 4.2.2.2):** Adopt the most desirable sector-specific certification based on customer demands.
- **Common Denominator (section 4.2.2.3):** Certify a common denominator of sector-specific security controls, ideally auditing once to comply with many standards.

- **All certifications (section 4.2.2.4):** Minimize audit overhead by acquiring all relevant certifications (as per customer demand) to satisfy the customers' security demands, regardless of the sector-specific nature or overlap with existing certifications.
- **Component certification (section 4.2.2.5):** A general organization-wide security baseline supplemented by specific in-depth product and/or process certification(s).

4.2.2.1 No certification (by an independent third party)

The **"No certification"** strategy is defined as refraining from acquiring certification by an independent third party and accepting additional audit overhead from customers themselves or their auditors. This strategy ought not to be misconstrued as not having any security measures or documentation in place. It is always essential to ensure an appropriate level of information security, regardless of certification.

This strategy effectively lowers the external auditing costs and increases internal auditing costs instead. Both IT auditors and technology providers supported this trade-off between external and internal auditing costs, stating: *"Not being certified does not mean an organization's security is necessarily flawed. The absence of third party certification lowers the external auditing costs, but simultaneously drives up internal auditing costs, because demonstrability is key. Even without certifications organizations often have to show transparency to their partners through for example a capability statement. Moreover, larger companies often perform a selection based on a request for proposal or request for information with certain certification or security demands."*

When opting to forego third party certification, an organization would have to endure continuous audits, which means having to hire additional compliance officers to accommodate audit overhead. It is the least scalable strategy, given the need for compliance officers proportional to the auditing demands. Moreover, customers that only work with certified organizations, due to regulatory requirements or organizational preferences, would be off-limits to the technology provider. Out of the four strategies, it offers the highest degree of flexibility, because it allows a technology provider to make any changes without requiring recertification or communication with auditing partners. However, not all interview participants agreed that this strategy necessarily offers the highest degree of flexibility. One of the IT auditors stated: *"I have audited and given out certifications for companies as little as 2 employees all the way to as many as 100.000 employees. Therefore, one cannot say that certifications necessarily impede flexibility. It simply means that the auditee must communicate any planned changes ahead of time with the IT auditor, who will reassess whether it is necessary to conduct a surveillance audit."* As such, when we state that this strategy makes an organization less flexible, we imply that it imposes certain bureaucratic processes that a technology provider must follow in order to maintain an acquired certification (such as communicating any major changes with the auditor in advance).

When speaking of no certification, we explicitly refer to certification given out by an independent third party. Several interview participants suggested the use of first party (self-assessment) or second party (associated assessment) certification. Both security officers and IT auditors reported, *"Pay careful attention to the use of self-reporting or second party certification. Sometimes it pays to utilize the services of a smaller startup even in the absence of third party certification. In such scenarios, we ask our own privacy or security related questions and conduct our own risk analysis."* These first and second party certifications (self-assessments and associated assessments) provide less assurance, but may be cost-effective alternatives for managing one's information security system and qualify as viable options for executing this strategy.

The context in which this strategy is most applicable depends on several factors, such as the type of regulations, number of customers and financial resources.

First, regulation plays a vital role. In the Netherlands, third party certification is rarely imposed by regulation. Exceptions are certain critical industries such as the healthcare sector, TSPs and telecommunication providers. However, national regulation determines the degree to which certification is imposed by regulation, meaning that there can be substantial differences between different countries. Several technology providers mentioned that organizations operating in the United Kingdom are required to have some form of an information management system (ISMS) in place, which practically implies an ISO 27001 certification. Another key variable is the number of customers of a given technology provider. This strategy is likely to be more beneficial when the number of customers is low, because internal auditing costs are likely to be much lower than the external auditing costs of acquiring certification from an independent third party. Under the presumption that most customers want to verify

their technology providers' information security, more customers indicate more auditing overhead. The lack of scalability comes from the proportional increase in auditing overhead according to the number of customers, eventually resulting in many time-consuming and repetitive tasks. At this point, any technology provider would be more likely to lower their total costs through the adoption of certification(s).

Access to capital ought not to be forgotten either. Adoption of appropriate certification may result in lower long-term costs in some situations, but given the necessary upfront costs, technology providers with limited resources may opt to postpone the acquisition of certification. As such, this strategy seems most suitable for startups with fewer financial resources and fewer (usually smaller) customers until the benefits of certification outweigh the relatively high up-front costs.

Overall, this concept seems most suitable for startups operating in the scenario of "few sectors, few customers" (the bottom left scenario in Figure 8).

4.2.2.2 Sector-specific certification

The **"Sector-specific certification"** strategy is defined as adopting the most desirable sector-specific certification based on customer demands. This is often the first step-up from not having any certification at all for technology providers that have started to gain more customers. It is rather straightforward to adopt the certifications that are most desirable and most relevant in a given sector, especially when the number of customers in that sector justifies the adoption of the appropriate information security standards as we have shown in Table 2 of section 4.1.1. Within-sector overlap is typically a rare occurrence and therefore, not much of a concern for most organizations. The reduction in audit overhead and the simultaneous bump in trust make this strategy a no-brainer for most technology providers looking to acquire their first certifications.

That being said, most technology providers would do well to consider the acquisition of an organization-wide ISO 27001 certification prior to pursuing other, more sector-specific certifications. Irrespective of sector, ISO 27001 has become the norm in Europe and may even be imposed by regulation in some cases. As mentioned in the previous sub-section (section 4.2.2.1), organizations operating in the United Kingdom are practically obliged to have an appropriate ISMS in place.

Overall, this concept seems most suitable for technology providers operating in the niche scenario of "few sectors, many customers" (the top left scenario in Figure 8).

4.2.2.3 Common denominator

The **"Common denominator"** strategy is defined as the construction of an individualized control framework according to the certification demands of a specific organization, where the goal is to incorporate the security requirements of multiple sectors into a set of sector-specific security controls, which we call the common denominator. This common denominator is then certified as a whole, leaving only a limited number of highly specific controls outside the certified scope. Essentially, this strategy can be characterized as "audit once, comply with many". Although this approach may not fully eliminate audit overhead, it is expected to reduce the audit time while minimizing the number of acquired certifications. It takes inspiration from Amazon's AWS approach as discussed in section 2.3.2.

However, certifications imposed by sector-specific regulation may impede its feasibility. Moreover, the construction of such a common denominator might be perceived as difficult, given the fact that it requires a comprehensive understanding of all relevant information security standards and how they relate to each other. In order to perform this strategy, it is necessary to map an organization's own security controls onto the different standards in order to identify the overlap and extract a common denominator. The term ''common denominator'' might seem to imply that one can only include identical controls that overlap across sectors. However, the common denominator is simply a collection of sector-specific security controls. As such, they do not necessarily have to overlap, giving the technology provider total freedom over the inclusion and exclusion of security controls.

Regarding potential pitfalls, it may not always be feasible to certify the common denominator under one accredited auditing scheme. As such, several participants mentioned the usefulness of utilizing a third party memorandum (TPM), which is a statement given out by a third party to provide assurance that an organization is compliant with a certain control framework. One standardization agency reported *"If the auditor is willing to cooperate, a TPM is less strict, because it is constrained by fewer rules. The tool kit is larger than just a certificate or no certificate, which offers flexibility. When operating in a complex*

environment, such as a large hospital, I believe one should construct a TPM, because the individual certifications are not catered to match such complexity." In addition, one of the technology providers reported that *"we have successfully implemented a common denominator through a broadly scoped SOC 2 assurance report and a separate TPM. It was a time-consuming process, but well worth the work. However, it is important to present these complex documents to those that have a solid understanding of the underlying standards, rather than those simply going through a compliance check-list."*

The keen reader of this thesis might point out that a TPM is technically not a certification, but an assurance report. We consider TPMs to be comparable to certifications in the context of this research project, given the fact that they are both utilized for the purpose of providing information security assurance in the context of technology providers. This is similar to the comparison between certifications and SOC 2 assurance reports, as described in the introduction chapter of this research (section 1.2). This control framework may very well be composed of the set of controls that makes up the common denominator. However, one ought to keep in mind that these TPMs are often less detailed and are not necessarily accompanied by matching accreditation, nor do they hold the same commercial power as recognized certifications (which are accompanied by appropriate accreditation). To overcome these concerns, technology providers could consider utilizing a more expensive broadly scoped SOC 2 assurance report as a TPM with recognized commercial power.

It is important to point out that not all participants were necessarily hopeful about the common denominator approach. Some showed skepticism and stated that *"it is a good idea, but might not be feasible on a larger scale, because it may put certain companies out of business."* One of the IT auditors reported that *"it is possible, but the problem is that the partners of a technology provider will have to compare the broadly scoped SOC 2 assurance report (or another kind of TPM) to their own certifications, which can prove troublesome in practice."* Overall, the majority of the participants did think that practical application of a common denominator was feasible in certain situations.

This concept appears most applicable when an organization deals with many standards, but has fewer customers. Essentially, it tends to act as a cost-effective middle ground solution that provides less overall assurance than accredited standards. The interview participants expressed interest in this strategy as a means of managing a large number of certifications, given that it stimulates technology providers to analyze their own security policies and relate these back to all the relevant information security standards.

Overall, this concept seems most suitable for technology providers operating in the niche scenario of "many sectors, few customers" (the bottom right scenario in Figure 8).

4.2.2.4 All certifications

The **"All certifications"** strategy is defined as adopting certification as needed in order to satisfy the customers' security demands, regardless of the sector-specific nature. Essentially, an organization would accept the fact that the certifications are likely to be accompanied by significant amounts of overlap with already acquired certification. It is often the most expensive strategy, which restricts its use to organizations with sufficient resources and enough customers to justify its costs.

However, this strategy does not imply that organizations blindly pursue any and all certifications simply because a customer requests to see a certain certification. It is essential that the technology provider still checks whether the desired certification is relevant for them in the first place. Nonetheless, this certification does not solve the inefficiency of certification overlap and still suffers from the chaotic nature of the certification landscape. Technology providers will have to put in the work to maintain a clear overview and not get lost in a jungle of certifications. Failure of doing so could possibly lead to what we refer to as legacy controls, where a lack of overview results in situations where it may no longer be clear which security controls belong to which certification, resulting in security controls that are outdated and possibly no longer relevant.

Although sub-optimal in most situations, this strategy does offer benefits. The interview participants reported that, out of all the strategies discussed thus far, it results in the highest possible reduction of audit overhead from the perspective of the customer. Both technology providers and IT auditors stated: *"Adopting all relevant certification eliminates the need for customers to perform their own audits on the technology provider, which allows for easy demonstrable compliance. However, the quick and easy*

compliance comes at the expense of higher complexity. The number of incidents is likely to go up, because every different auditor is likely to come up with his or her own findings. Moreover, the overview of all the relevant standards and frameworks will become more complex and require better certification management All of this might result in an overall increase in the time-to-market, because every major change must first be communicated with the audit partners (and potentially impose a surveillance audit)."

As such, additional certification is still accompanied by one or more audits from independent parties and adds to the overall complexity of certification management. In addition, technology providers with sufficient financial resources may opt to pursue certifications beyond the minimum requirements as a means of distinguishing themselves from competitors. Interview participants from all stakeholder groups emphasized the utility of certifications as a unique selling point, rather than just mandatory compliance.

This strategy is primarily utilized in scenarios in which a technology provider has a large number of customers per sector. Moreover, going beyond the minimum certification expectations can be utilized to achieve a competitive advantage in luxury markets where competition is fierce. On the other side, additional certifications must be earned back one way or another, potentially driving up the price of a product or service.

Overall, this concept seems most suitable for technology providers operating in the most complex scenario of "many sectors, many customers" (the top right scenario in Figure 8).

4.2.2.5 Component certification

The **"Component certification"** strategy is defined as a general organization-wide security baseline supplemented by specific in-depth product and/or process certification(s). Currently, most of the commonly adopted certifications are created based on sector-specific regulations, which apply to the whole organization, rather than only the relevant areas for a given product/service. This is because they are not catered to the use of widespread outsourcing and sub-contracting. Component certification could theoretically ease up on the continuous auditing demands by reducing the size of existing certification, because it divides existing certification schemes into smaller individual modules that are no longer confined to specific sectors or industries. As such, this would result in certifications with a narrower but more specific scope and the sector nonspecific nature could reduce the total number of sector-specific certifications. Component-based certification may result in smaller, less complex certification schemes. Component certification could effectively shift the focus from certification based on sector-specific regulation to certification based on competence.

All the interviewed technology providers showed tremendous interest in the concept of modular certification, given that they are ones who are primarily confronted with the inefficiencies of the current certification process. Moreover, one of the IT security experts mentioned: *"I think it is almost inevitable that we will eventually evolve into a modular certification approach. The world continues to develop in the direction of specialization and specialized service-based IT. We see a surge in the degree of outsourcing to specialized third parties, because we truly need their expertise. It would be impractical, if not impossible, to acquire the highly specialized knowledge without relying on outsourcing. If we handicap cooperation between specialized parties, it will come at the expense of innovative opportunities."*

However, participants did voice concerns regarding its feasibility and finding IT auditors that are both capable and willing to facilitate component certifications in the current market. In addition, certain IT auditors could be opposed to the idea of component-based certification for several reasons. First, it might take work out of their hands. The number of certifiable certifications may decrease and therefore, so will the demand for the number of yearly audits. If the demand for audits is greater than what an auditor can cope with, this may be beneficial, but less demand for IT audits is more likely to be considered a threat to the IT auditor. Moreover, a modular approach can only function if IT auditors are willing to trust each other's work, which may prove troublesome in practice. Regarding IT auditor cooperation, one security expert stated: *"From my experience, auditors will be cooperative as long as the customer requests them to."* Another IT auditor mentioned: *"In particular from the perspective of ISAE, auditors are required to rely on a certification or assurance report given out by a different auditor."* In contrast, both a technology provider and an IT auditor mentioned that they think it might be wishful thinking, stating: *"We continue to see new standards and frameworks emerge. In particular, we see a reinvention of the wheel happening in the field of privacy certifications with nearly identical controls.*

Perhaps in part, because the development of standards is a business model for standardization agencies. Regulation might from higher up might be able to aid in overcoming some of these issues."

On the other hand, in the systematic literature review we have shown that some of the common challenges associated with information security certification are related to the complexity of the IT audit and the reliance on individual IT auditor competence. We argued that the quality of information security certification is multifactorial and not easily captured in a single framework. Regarding IT auditor competence, we stated that *"it appears that the inadequate security assurance can be explained by the genericity of large frameworks, a lack of standardized methodology and limited IT audit guidance. This shifts a significant portion of the responsibility to the IT auditors, resulting in individual auditor competence to be a critical factor in contributing to the success of IT audits"* [3].

In addition, the interview participants in this research project reported similar findings to our conclusion from the literature review. Several IT auditors and one standardization agency elaborated on the issue of IT audit complexity and stated: *"The level of complexity is constantly rising. We see this in the eIDAS area, where we have exactly this situation that the operation of a trust service provider can become so complex that the TSP already starts outsourcing tasks to specialized companies. That becomes the driving force behind a component audit. As long as both the industry and technology develop, a normative body will eventually set up a corresponding normative set of requirements. However, the industry continues to develop their products even further, increasing the level of complexity, resulting in a situation where the normative agencies have not yet addressed these newer developments. It is a question of synchronization of tasks."*

In theory, component certification can contribute towards addressing these issues, but it brings up the topic of feasibility. One of the interviewed IT auditors stated: *"At the moment,* m*y feeling is that component certification is a kind of intermediary tool that we are using until the weight on this side of the scale is large enough for the normative body to start working on a specific norm. That is what is currently happening in the area of identifications."* Although the TSP and telecommunications industry is currently the only sector utilizing a modular approach, other industries have certainly recognized its potential. In 2018, the European Network and Information Security Agency (hereinafter ENISA) published a report on the topic of European ICT security certification in the healthcare sector in which they stated: *"Traditional standardisation processes, however, can be time-intensive, potentially causing delays in the application of necessary standards and interoperability."* They went on to conclude: *"It is impossible to certify the healthcare sector as a whole… A solution to overcome this situation would be to establish a segregated scheme, providing links between other schemes. Synergies across various "certifiable" areas should be used to a large extent to reduce the amount of similar certification approaches"* [35].

Regarding the context in which component certification could be applied, the participants mentioned that a modular approach is particularly useful in situations where an organization operates in several sectors. This is especially the case when the number of customers per sector is relatively low, given the high upfront costs associated with the acquisition of information security certifications. Another key factor is the degree in which sector-specific standards overlap with each other, with higher degrees of overlap increasing the usefulness of a modular approach. Lastly, component certification requires interoperability between different certification components and auditing schemes.

Overall, this concept seems most suitable for technology providers operating in many sectors, regardless of the number of customers. In other words, the right side of Figure 8 (either the top or the bottom right scenarios). However, the participant responses appear to be divided, which leads us to conclude that the qualitative interview data on component certification remains inconclusive with serious feasibility concerns.

4.2.3 General optimization practices

The strategies discussed in the previous section (4.2.2) are applicable in specific contexts and are characterized by a relatively high degree of mutual exclusivity. In this section, we introduce four additional concepts, which we refer to as general optimization practices. These practices are defined as *a set of good practices* that can be used in conjunction with the certification strategies presented in the previous section to support certification processes and results in more efficient certification management.

Unlike the strategies in section 4.2.2, the general optimization practices are applicable in a wider context and are much less mutually exclusive. Technology providers can incorporate multiple optimization practices on top of the certification strategies to improve the efficiency of the certification process. Although the supplementary use of these general optimization practices is not restricted to a specific certification strategy, they appear to be most beneficial in situations where a technology provider operates in multiple sectors, which is the right side of the certification lifecycle in Figure 8.

We introduce the following four general optimization practices that are useable in conjunction with the previously defined certification strategies:

- **Parallel audits (section 4.2.3.1):** Simultaneously conduct several audits of different information security standards to avoid having to endure repetitive audits.
- **GRC tooling (section 4.2.3.2):** Utilize Governance, Risk & Compliance tooling to reduce the complexity and improve the efficiency of managing certifications.
- **Diversify certifications into sub-components (section 4.2.3.3):** Diversification of acquired certifications by splitting them up into several smaller sub-components with their own separate scopes.
- **Leverage certifications in negotiations (section 4.2.3.4):** Leverage the reduction in audit overhead due to the acquisition of appropriate certification to assume a favorable negotiation position.

4.2.3.1 Parallel audits

This concept is defined as simultaneously conducting several audits of different information security standards to avoid having to endure repetitive audits. This was the most suggested concept among the interview participants, which is why it appears to be a promising solution. Parallel audits can be conducted by a team of auditors (often referred to as team audits) or by a single auditor with accreditation (if necessary) for several security standards. Parallel audits are often performed by a single competent auditing agency, but could also be performed by several auditing agencies, as long as these auditors are willing to cooperate with each other. In such a scenario, transparency and agreements among the auditors is essential. Several interview participants in the role of IT auditors commented on the usefulness of these audits, stating: *"Reusing certification does not work, but the practical lesson or solution is to search for an auditor that is skilled and accredited to audit several areas of interest at the same time (team audits). Then you cluster different audits with one auditor (company). This auditor might come along with other specialized partners who support audits that the individual auditor might not have in its portfolio, in order to overcome the problem of acknowledging results that you have not gained yourself."*

The IT auditors went on to share their own experiences with conducting parallel audits, stating: "*We did this together with my colleague. We selected the area where we have an overlap and defined the audit schedule in a way that all auditors looking at the same contents were present in the same audit sessions relevant for them. The outcome is an audit schedule that is tailored in the way that every auditor received the information he or she needs in the sessions they need to be present in. As a result, the auditee was faced with the situation where they could run the audits in parallel. We did it in one batch simultaneously, instead of four audits in sequence over several months. That only worked, because we did it under one roof and involved auditors from the same company. It was possible to exchange the relevant information between the auditors and share the knowledge to come to an output. Based on a very similar set of questions we issued various certificates. The clue here for the company under audit is to carefully look at the partner they are selecting and ensure that the partner is knowledgeable, experienced and skilled to do that."*

Given the above statement, we conclude that parallel audits are particularly useful in the context of technology providers looking to be certified for several certifications or are expected to do so in the near future and that partially overlap (such as ISO 27001 and eIDAS/ETSI and SOC 2). Proper auditor partner selection is key, given the likelihood of engaging in a long-term partnership. Moreover, not all auditors are capable and/or willing to conduct these types of audits, given the huge increase in workload on the side of the auditor and the increased level of complexity associated with these types of audits (as explained by interviewed IT auditors). Auditor competence is crucial, because it is likely that a single lead auditor will be responsible for the majority (if not all) of the certifications. Parallel audits effectively eliminate a significant number of repetitive work that would otherwise be performed by other auditors.

Although this mitigation of relatively redundant tasks is invaluable, its consequence is that a given auditor's work is less likely to be examined by another auditor.

Finally, on the surface, it might seem that parallel audits are an effective method to drive down the auditing costs. However, this may not necessarily be the case for every situation. The IT auditors that had experience in conducting parallel audits stated: *"Keep in mind that team auditing is something which is not standardized. It depends on the qualification of the auditor you are choosing, the willingness of the auditor and on the auditor's side, there is probably nothing which would produce much savings. Auditors have the additional work of sketching the overlap and organizing everything to make it happen in the end. It should be kept in mind that the auditor really tailors the audits specifically to the auditee's needs."* As such, the complexity of parallel audits ought to be considered when determining whether or not parallel audits (or team audits as the interview participants phrased it) provide a meaningful benefit in a specific context. Overall, we do believe that parallel audits would result in lower long-term auditing costs when compared to acquiring the same certifications sequentially. However, one might consider it a trade-off between higher up-front costs, but lower long-term costs. The company under audit would do well to carefully consider the selection of an appropriate audit partner and extensively evaluate which certifications ought to be acquired (and in what order they ought to be audited).

4.2.3.2 GRC tooling (Governance, Risk & Compliance)

Several interview participants brought up the topic of utilizing Governance, Risk & Compliance (GRC) tooling for reducing the complexity and improving the efficiency of managing certifications.

In a recent study on the role of GRC in the field of information systems, Papazafeiropoulou described GRC tooling as: *"GRC software enables an organization to manage the GRC-related enterprise strategy following a holistic approach. A single framework is provided integrating the three aspects of GRC acronym together, supporting the administrators in monitoring and enforcing rules and procedures"* [36]. As such, GRC tooling aids in the management of information security management system (ISMS), including the management of security standards and certifications.

The GRC tool supplier interviewed for this research project revealed that GRC tooling could aid in several ways:

- Highlight overlap among standards: The supplier stated: *"We are capable of indicating the degree of overlap among different information security standards by mapping controls of relevant security standards and certifications onto each other."*
- Integration of risk analysis, vulnerability assessments and task management: The supplier stated: *"To promote efficiency of processes, we automate certain processes, such as generating compliance statements, auditing reports, updating standards and communication with external applications."*
- Certification management & monitoring: The supplier stated: *"We track the duration of time for which certifications are valid and remind our customers when it is time for a surveillance audit or when a certification approaches its expiration date. This essentially prevents outdated standards or so-called legacy controls and reduces the complexity."*
- Deliver graphical dashboards: The supplier stated: *"We provide a clear overview through graphical dashboards, which aids in the planning process. We offer several types of dashboards, including ones that display the entire internal audit cycle. These dashboards are capable of showing the degree to which a set of controls is compliant with one or more security standards."*
- Provide integrated e-learning systems: The supplier stated: *"We have integrated systems for different frameworks that generate reports with details such as vulnerabilities, employee risk awareness and the degree to which one is compliant with a standard."*

When discussing GRC Tooling, we have to touch on the so-called "GRC versus IRM" debate as well. In 2017, John Wheeler and Gartner (a large consultancy firm) claimed that GRC had become outdated and introduced their own Magic Quadrant for Integrated Risk Management (IRM). Wheeler argued that GRC is considered to be more of an organization-wide strategic decision, whereas the concept of IRM was defined as *"a set of practices and processes supported by a risk-aware culture and enabling technologies, that improves decision making and performance through an integrated view of how well an organization manages its unique set of risks"* [37]. Since then, the concepts of GRC and IRM have been compared and debated heavily, but it remains unclear to the author of this thesis as to what exactly

sets them apart from each other. Some would even argue that the discussion appears to be based on politics, rather than the introduction of an industry-changing concept.[19] As such, for the sake of this thesis, we consider GRC and IRM sufficiently similar to treat them as comparable and include IRM as a more specific and cost-effective type of GRC tooling.

The GRC tool supplier interviewed in this research stated: *"IRM is simpler, faster and cheaper than GRC tooling, making it better suited for SMEs with a smaller budget. GRC tooling is more expensive and suited for larger enterprises. As such, our software solution should be considered as an IRM tool, suitable for smaller organizations. Our solution is an affordable and highly-specific ISMS with a relatively fast implementation time, whereas conventional GRC Tooling tends to be larger (less specific), more expensive and comes with a longer implementation time."* The main takeaway is that it appears that there are solutions in all shapes and sizes for organizations in different situations. Annual costs can range from as little as under €5.000 (which we consider to be more in line with the concept of IRM) to over €200.000 (which we consider in line with more traditional GRC tooling) with similarly pronounced differences in terms of implementation times. The primary benefits are considered to be increased efficiency and reduced complexity, which may allow for a smaller compliance department and better management of certifications.

Although GRC tooling can be regarded as a general optimization practice, its added value depends on the context. When a technology provider comes into contact with a limited number of certifications (such as in the context of operating in few sectors), the benefits of GRC tools are unlikely to outweigh the costs and learning curve. As the complexity of managing certifications and security standards increases, so does the added value of GRC tooling. However, one ought to consider that management of certifications does not necessarily have to fall under the responsibility of the technology provider (auditee).

When incorporating parallel audits as described in the previous sub-section, it makes sense to utilize the expertise of the auditors to aid in managing activities such as mapping the controls of different standards onto each other to indicate the degree of overlap among standards. If the auditor already takes responsibility for such tasks, additional use of GRC may yield fewer benefits. As such, when the technology provider is responsible for the management of its own certifications, the need for GRC tooling may be higher. However, when the auditor covers a significant portion of these tasks, one should take this into consideration when evaluating the added value of incorporating GRC tooling.

4.2.3.3 Diversify certifications into sub-components

By far the most situational practice, large enterprises may consider diversifying their acquired certifications by splitting them up into several smaller sub-components with their own separate scopes. According to one of the IT security experts *"splitting up a large certification into smaller subsets with their own scopes might be worth considering in situations in which a corporation wishes to employ several information security management systems (ISMS)"*. For example, organizations operating in several countries, or organizations responsible for a variety of products and/or services, may opt to spread certifications out across smaller branches, countries or areas of operations.

The primary benefits of this would be to reduce one's dependency on one broadly scoped certification, which results in a subset of several smaller certifications with their own scopes. These smaller individual scopes are less complex and easier to maintain. However, the obvious downside is that it increases the total number of acquired certifications and therefore, potentially drives up the total certification costs. Moreover, it may incur more repetitive work, because all the smaller individual scopes have to be certified individually.

4.2.3.4 Leverage certifications in negotiations

This optimization practice is defined as leveraging the reduction in audit overhead due to the acquisition of appropriate certification to assume a favorable negotiation position by showing that customers mutually benefit in the form of cost reductions. When a technology provider is certified accordingly, the customers can rely on the validity of a certificate issued by an independent auditor and therefore, will no longer have to conduct audits on the technology providers themselves (or at the very least, reduce the time spent conducting their own audits). If technology providers are aware of this, they can potentially recover part of the certification costs through leveraging these benefits in contractual

[19] https://central.co/the-story-of-grc-vs-irm/

negotiations with customers in order to charge customers for maintaining the desired certificates. This, in turn, can improve the scalability of certification in general, allowing technology providers who would otherwise be unable to overcome the certification entry barriers to establish appropriate partnerships.

That being said, this practice cannot be employed by just any technology provider. Several IT security experts reported: *"Whether or not certifications can be leveraged to obtain a favorable negotiation position, strongly depends on the degree to which a technology provider's product/service is easily replaceable by a competitor. Both an organization's technical expertise and reputation play an important role."* As such, reputable technology providers may be able to leverage a stronger negotiation position when discussing pricing options. Moreover, technology providers would do well to consider possible renegotiation as the number of acquired certifications expands.

4.2.4 Strategies in perspective: Our comparison

This section puts the strategies that were discussed thus far in perspective. Section 4.2.4.1 introduces a novel certification strategy selection framework (depicted in Figure 9), in which we provide a graphical representation of the concepts composing this framework by showing the context in which the various strategies are likely to be reasonable strategies. Section 4.2.4.2 summarizes the advantages and disadvantages of the five strategies and four optimization practices into one comprehensive overview (depicted in Table 4).

4.2.4.1 Strategy selection framework

The goal of our newly proposed certification strategy selection framework is to support the security certification stakeholders and the decision-makers in identifying and evaluation their available options.

Figure 9 introduces a certification strategy selection framework based on our interpretation of the data. It provides a visual comparison of the concepts that were discussed thus far and consists of a four-quadrant matrix that we adapted from the technology provider certification lifecycle (Figure 8 in section 4.2.1), as well as a set of supplementary optimization practices. The certification strategies introduced in section 4.2.2 are mapped onto the four distinct quadrants. Many of these strategies are mutually exclusive, which is why most scenarios (quadrants) contain a single strategy. The remaining four general optimization practices, introduced in section 4.2.3, are mapped onto the highlighted green area, indicating their additive benefits.

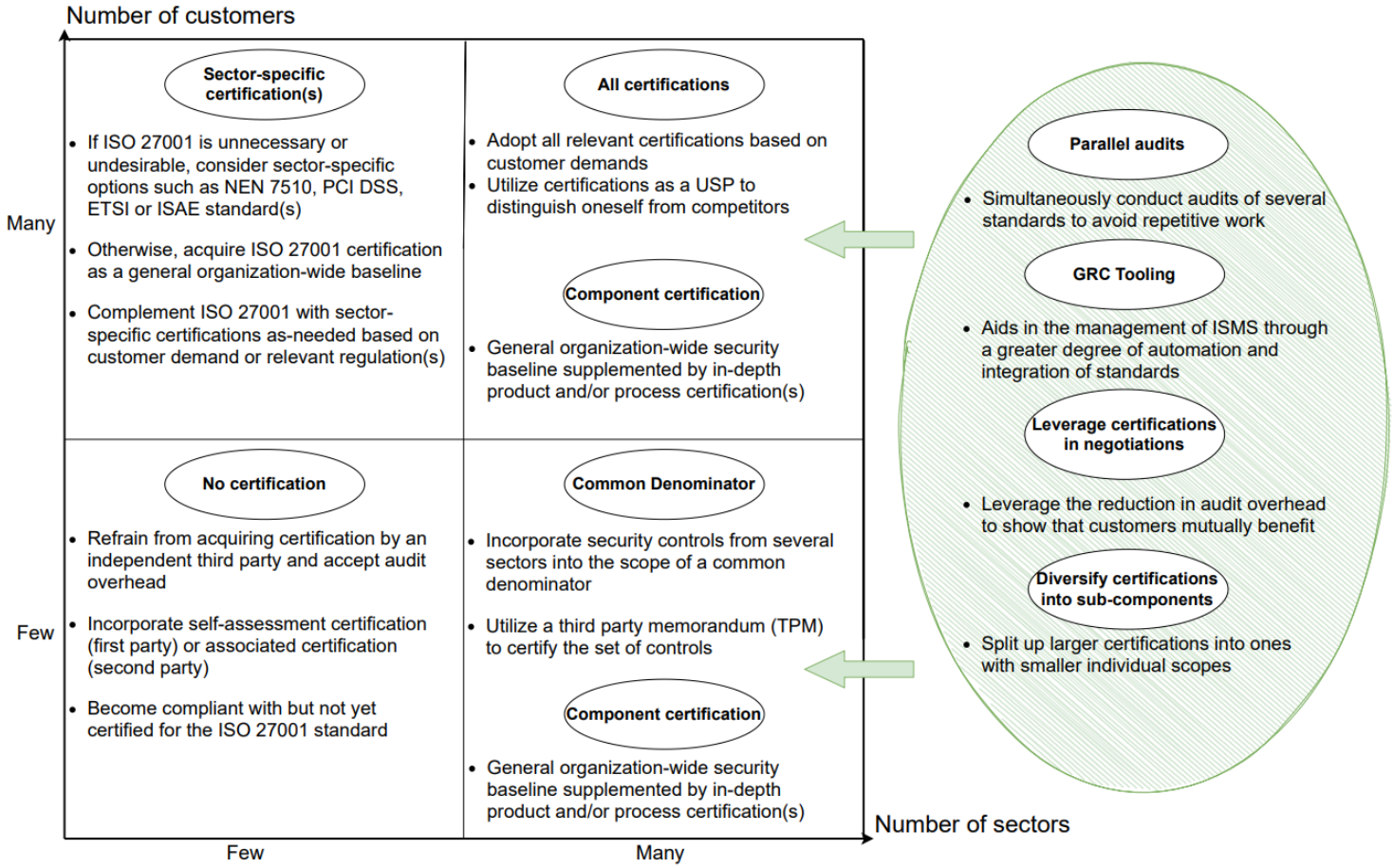

Figure 9: Certification strategy selection framework.

The bottom left scenario (few sectors, few customers) is typically characterized by startups in the earliest phase of their certification lifecycle. This scenario is limited in its options, as it is constrained by its lack of resources. Essentially, the only option is to *forego certification and endure audit overhead until the benefits of third party certification outweigh the costs*.

The subsequent scenario located directly above it in Figure 9 (few sectors, many customers) is characterized by a slightly higher degree of choice. As the number of customers per sector is relatively high, resources ought to be sufficient and the benefits of third party certification are likely to outweigh their costs, hence the *adoption of sector-specific certifications.* However, it is important to point out that we include ISO 27001 in this scenario in spite of the fact that its primary characteristic is its cross-sector applicability as a general organization-wide information security baseline. We do this, because in most situations ISO 27001 might be the only certification that is required of a technology provider, even if their services are confined to a limited number of sectors (sometimes imposed by regulation, other times because of customer demands). That being said, there can certainly be situations in which a technology provider is not required to have ISO 27001 certification to satisfy its customers' security demands or to comply with regulation(s). For instance, if a given technology provider is confined to operating in the Dutch healthcare sector, NEN 7510 certification might just suffice on its own.

Moving on, the bottom right scenario (many sectors, few customers) is characterized by SMEs that have started to expand their core business to a wider scope, i.e. across sectors. Therefore, this scenario is a suitable candidate for the *common denominator* approach. Given the relatively high number of relevant standards, organizations may wish to reduce the audit overhead through a TPM for several sector-specific controls. Given the relatively low number of customers, financial resources are still limited, making it difficult to adopt a significant number of certifications. Certifying a common denominator of sector-specific controls can be a cost-effective middle ground solution. If available, applicable and affordable, *component certification* also starts to become relevant, given the lesser degree of overlap resulting in a more efficient and less repetitive audit.

The last scenario, located at the top right (many sectors, many customers), is the most complex and demands the organization's highest commitment to certification management. Organizations typically range from middle-sized companies to large enterprises. In this scenario, technology providers can opt to *adopt all relevant certifications*, which significantly reduces audit overhead, but conversely induces complexity through increasing the demand for managing the acquired certifications. Similar to the previous scenario, *component certification* would be an ideal concept, but given its limited practical applicability in the current industry, it does not suffice on its own.

Finally, the highlighted green area contains the general optimization practices as discussed in section 4.2.3. Contrary to the five certification strategies, these optimization practices are not necessarily mutually exclusive and might be combined to achieve a synergistic effect depending on the context. The general optimization practices are particularly relevant whenever a technology provider operates in many sectors, depicted by the green arrows pointing to the right half of Figure 9. These practices facilitate information security standards across several sectors. As such, they are characterized by cross-sector applicability, regardless of the number of customers (and are applicable in both the bottom and top right scenarios).

4.2.4.2 Advantages & disadvantages

To conclude this section, the advantages and disadvantages of the five strategies and four general optimization practices have been summarized. The findings were condensed into a comprehensive overview and are presented down below in Table 4 on the next page. Both the strategy selection framework (Figure 9) and the findings from Table 4 function as a steppingstone towards the development of the artifact of this research, which is introduced in the next chapter.

Strategy/ Optimization practice	Definition	Advantages	Disadvantages
No third party certification	Refrain from acquiring certification by an independent third party and accept additional audit overhead	• Low external auditing costs • High flexibility	• High internal auditing overhead and costs • Not scalable
Sector-specific certification	Adopt the most desirable sector-specific certification based on customer demand	• Less audit overhead	• Limited cross-sector applicability
Component certification	A general organization-wide security baseline supplemented by specific in-depth product and/or process certification(s)	• Highest reduction in audit overhead • Cross-sector applicability • Less complex audits and smaller audit schemes	• Confined to ETSI and ISO standards • Possible conflicting stakeholder interests • Requires interoperability between certification schemes
Common denominator	Certify a common denominator of sector-specific security controls, ideally auditing once to comply with many standards	• Cost-effective cross-sector compliance • Audit once, comply with many standards	• Less assurance than accredited certification • Construction of common denominator is labor-intensive • TPMs might not be recognized by customers
All certifications	Minimize audit overhead by acquiring all relevant certifications) to satisfy the customers' security demands	• Highest reduction in audit overhead • Utilize certifications as a USP to distinguish from competitors	• Highest degree of complexity • High risk for overlap and repetitive tasks • Cost-prohibitive • Reduced flexibility
Parallel audits	Simultaneously audit multiple standards to decrease the degree of repetitive audits	• Less repetitive work • Less audit overhead and costs	• IT auditor selection can be difficult • Risk of potential lock-in with IT auditor
GRC tooling	Utilize GRC tooling to decrease complexity and increase efficiency of managing certifications	• Reduces complexity • Improves efficiency • Enables smaller compliance department • Easier compliance	• Potential for lock-in once a vendor is selected • Requires migration of processes to GRC tool • Incurs fixed costs • Risk for dependency on a tool
Leverage certifications in negotiations	Leverage the reduction in audit overhead to assume a favorable negotiation position	• No additional costs • Benefits price negotiation	• Efficacy depends on reputation and degree of competition
Diversify certifications into sub-components	Diversify certifications into several smaller sub-components with their own separate scopes	• Reduces dependency among ISMS certifications • Smaller certification scopes • Enables diversification of certification strategies in the context of larger decentralized organizations	• Potentially higher costs and more repetitive work • Higher number of certifications

Table 4: Advantages and disadvantages of the certification strategies and optimization practices.

5 Maturity model

This chapter presents the main artifact delivered through this research project. We opt to put the findings of the previous chapter into perspective by expanding the selection framework to include optimization of one's information security certification processes within a given scenario. This is accomplished by combining the findings presented thus far into a novel certification maturity model, which is presented in this chapter and forms the main artifact of this research project. Section 5.1 explains the concept of maturity models and section 5.2 introduces a novel certification maturity model based on the findings from the previous chapters.

5.1 Background on Maturity Models

Maturity models have been introduced over the last four decades as guides and references for the management of information system in organizations from different sectors [38]. For the purpose of this work, we have chosen to adopt the definition by Blondiau et al. (2016), who define maturity models (abbreviated as MMs in the literature) as *recognized tools for demonstrating the gradual and systematic development and/or improvement of an organization's general skills, processes, structures or conditions* [39]. Maturity models can be leveraged to help organizations manage challenges such as rapid technology changes, mergers and acquisitions, increasing globalization or even structuring good project management practices. A maturity model is an indicator of progress that supports the identification of potential weaknesses, but does not automatically translate into organizational improvement [40]. They merely demonstrate how a given approach has been evolving, allowing organizations to enhance the planning of actions that should lead to the desired results and provide an effective way of measuring their processes [38].

Maturity models tend to follow a certain general architecture. Critical to any maturity model is the concept of maturity levels, which are predefined levels that specify certain characteristics. These characteristics are then evaluated to identify the appropriate organization-individual maturity level [41]. Higher maturity levels translate to a higher maturity of the underlying object under observation. In addition, maturity models contain several discrete stages that are assessed based on these maturity levels, resulting in a typical evolution path.

One of the earliest and the best known maturity models is the Capability Maturity Model (CMM), which was first developed to measure the maturity of software development practices and has inspired the development of many other maturity models [42]. Although the CMM was confined to the boundaries of software engineering, nowadays maturity models are applied to other fields as well [43]. Last year, Rabii et al. (2020) conducted a systematic literature review on the topic of information and cybersecurity maturity models and identified at least 20 different maturity models to-date [44]. In our own systematic literature review conducted in preparation for this thesis, we briefly discussed COBIT (Control Objectives for Information and Related Technologies) as one of the prominent IT governance frameworks [3]. Interestingly, COBIT also specifies its own generic maturity model, which incorporated the original CMM's six distinct maturity levels ranging from zero (non-existent) to five (optimized). The original CMM is depicted in Figure 10 on the next page. We present this model for illustration purposes, to indicate the meaning behind the maturity concept and its characteristics to readers of this thesis.

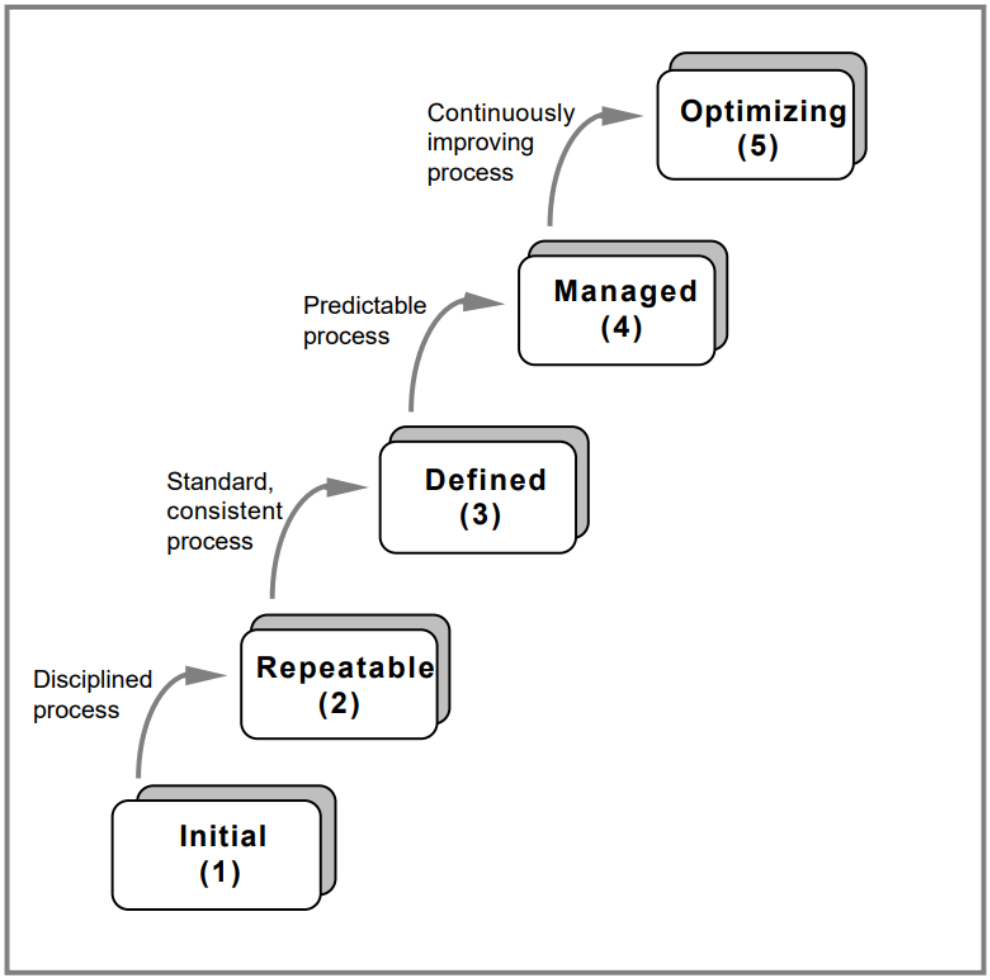

Figure 10: Capability Maturity Model (CMM) [42].

As briefly mentioned earlier, the five maturity levels outlined in the original CMM (see Figure 10) were designed for the field of software engineering and are defined as follows [42]:

1. Initial → The software process is characterized as ad hoc and occasionally even chaotic. Few processes are defined and success depends on individual effort.
2. Repeatable → Basic project management processes are established to track cost, schedule and functionality. The necessary process discipline is in place to repeat earlier successes on projects with similar applications.
3. Defined → The software process for both management and engineering activities is documented, standardized and integrated into a standard software process for the organization. All projects use an approved, tailored version of the organization's standard software process for developing and maintaining software.
4. Managed → Detailed measures of the software process and product quality are collected. Both the software process and products are quantitatively understood and controlled.
5. Optimizing → Continuous process improvement is enabled by quantitative feedback from the process and from piloting innovative ideas and technologies.

5.2 Certification Maturity Model

In chapter 4 we introduced the concept of a technology provider certification lifecycle (see Figure 8 in section 4.2.2). Furthermore, five certification strategies and four optimization practices were constructed and mapped onto the certification lifecycle (see Figure 9 in section 4.2.4). In this section we combine the findings of the previous chapters to introduce a novel certification maturity model (see Figure 11) in the context of technology providers, complemented by a set of good practices within the scenario in which a technology provider operates.

Our model is inspired by the original CMM and was designed through a top-down approach as defined by Mettler [45]. In line with Mettler's approach, we first defined the maturity levels, which were adapted from the CMM and then mapped these levels onto the field of information security certifications. It is structured as a prescriptive model and serves two purposes. First, we expect it to be able to indicate how technology providers can improve the maturity of their own information security certification strategies to positively affect the value of the business and/or processes. Second, we expect it to help in the decision-making process when considering an appropriate strategy for acquiring new certifications and managing existing ones. In other words, our proposed MM is supposed to aid organizations with the construction of a certification development roadmap.

Additionally, we separate maturity levels by focus areas (denoted by the scenarios displayed on the horizontal axis) and ordered these domains from the least mature to the most mature, resulting in an incremental development path (see Figure 11). We define the term ***maturity*** as the degree to which certification processes are structured such that a technology provider can satisfy its customers' security demands. The four strategies and five optimization practices that were introduced in this research were mapped onto the following six maturity levels, which are adapted from the CMM and defined as follows:

0. Non-existent → No certification is present, but might involve informal structuring of processes.
1. Initial → First certification is acquired, but no standardized processes are in place.
2. Repeatable → Cross-sector compliance is achieved, but lacks depth.
3. Defined → Standardized certification procedures, but a high degree of complexity.
4. Managed → Reduced complexity through incorporating an individualized approach.
5. Optimized → Processes are structured such that overlap among certifications is mitigated and certifications provide meaningful contributions on top of each other. Moreover, the technology provider actively participates in the development of information security standards.

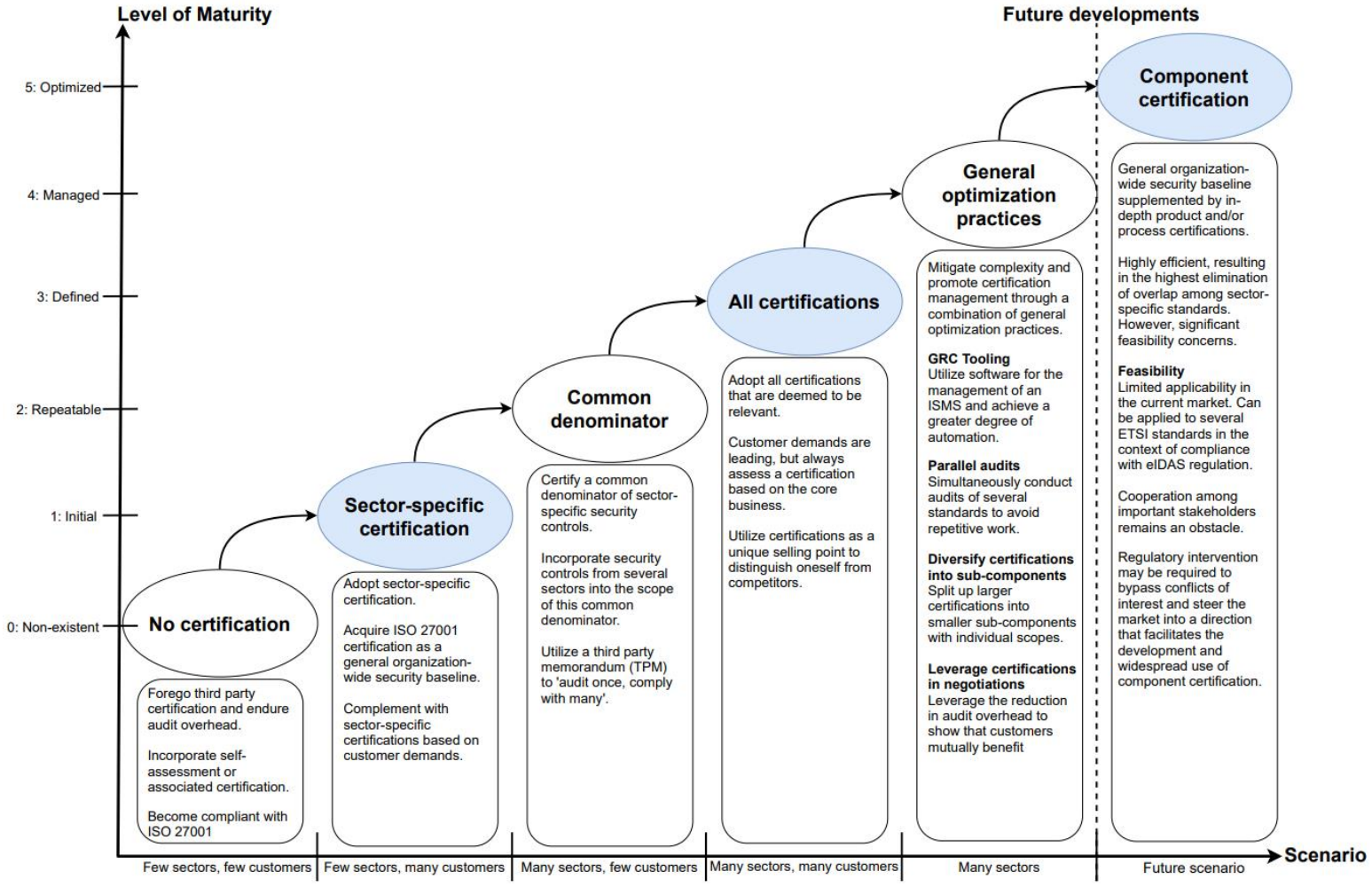

Figure 11: Certification maturity model.

The maturity model, depicted in Figure 11, indicates how technology providers can improve the maturity of their information security certification strategies to positively affect the value of the business and supports the decision-making process. The model shows a high-level overview of certification maturity in general and provides guidelines for maximizing maturity within a given scenario. Higher maturity is not always better, as the desirable maturity level depends on the situation. The horizontal axis depicts the different scenarios that we introduced in section 4.2. The vertical axis depicts six (including level zero) maturity levels that we adapted from the original CMM. Four out of the five certification strategies (introduced in section 4.2.2) are presented in the first four scenarios, followed by the general optimization practices (introduced in section 4.2.3). Finally, the model ends with the final remaining certification strategy (component certification) as a potential candidate for maximizing maturity in the future.

The maturity model follows the certification lifecycle as we described in section 4.2.1 (Figure 8). From a business perspective, startups tend to start out in the first scenario (few sectors, few customers) and aim to grow into the fourth scenario (many sectors, many customers). Although it is certainly possible to remain a niche, we argue that business drivers such as increasing market share and higher revenue are powerful drivers for facilitating growth from a business perspective, inevitably driving most technology providers to grow out of the immature scenarios on the left half, towards the more mature scenarios on the right half of Figure 11.

Progressing alongside the scenarios on the horizontal axis is likely to result in an increase in revenue, but also comes with an increase in the audit burden and audit overhead on the organization. From a business perspective, “many sectors, many customers” is the most lucrative scenario to be in. However, this scenario simultaneously calls for structured certification processes and requires proper certification management to mitigate complexity. As such, it is important to consider that Figure 11 essentially incorporates maturity from a high-level business perspective, but also provides guidelines within a given scenario for optimizing maturity on a certification level.

Facilitating efficiency and/or mitigating complexity is where the general optimization practices provide value. When a technology provider is certified for one or more certifications, these optimization practices can be utilized in conjunction with any of the certification strategies to optimize the maturity within a given scenario based on the individual organization. Proper application of these practices is likely to result in a more efficient and less complex management process. Finally, it is worthwhile noting that component certification is estimated to result in the highest level of maturity, but we list it as a potential future candidate due to its feasibility concerns and limited applicability in the current state of the market.

In the remainder of this section, we explain each individual scenario and provide our own suggestions for maximizing maturity within a given scenario. These suggestions are a manifestation of our interpretation of the qualitative interview results, as discussed in chapter 4 of this thesis.

Few sectors, few customers
This scenario is characterized by a lack of resources, effectively ruling out the possibility of acquiring certification by an independent third party. This essentially shifts the focus from certification management to proper management of audit facilitation to minimize the time spent enduring audits. To maximize maturity, we suggest the following good practices:

- Construct a compliance package to ensure that the process of enduring audits is as smooth as possible (proper documentation of internal security structure, predefined screenshots to show to the auditors etc.).
- Utilize first party (self-assessment) or second party (associated) certification as a cost-effective way to evaluate the internal control measures.
- Consider setting up the general processes such that the organization is compliant with, but not yet certified for the ISO 27001 standard to promote safety and prepare the organization for future certification.

Few sectors, many customers
This scenario frees up enough resources to justify the acquisition of third party certification. Given the relatively small number of sectors, it is reasonable to opt for the commonly adopted sector-specific standards. To maximize maturity, we suggest the following good practices:

- If ISO 27001 is unnecessary or undesirable, consider sector-specific options such as NEN 7510, PCI DSS, ETSI or ISAE standard(s).
- Otherwise, acquire ISO 27001 certification as an initial general information security baseline and complement with additional sector-specific options as needed.
- When opting for additional certification(s), consider at least the following factors:
    - Customer demand.
    - Relevant regulation.
    - Cross-sector applicability for potentially expanding to additional sectors in the future.
    - When opting for multiple certifications, consider choosing an IT auditor capable of granting a variety of certifications.

Many sectors, few customers
This scenario poses significant certification entry barriers for many technology providers. As such, the common denominator approach can pose as a cost-effective middle-ground solution for complying with several sector-specific standards. Although it may not be accepted by all customers, the certified common denominator may shorten the time spent enduring audits. To maximize maturity, we suggest the following good practices:

- Analyze all relevant sectors in which a technology provider operates to construct a common denominator, which is defined as a set of sector-specific security controls that occur across several sectors.
- Utilize a third party memorandum (TPM) to certify this common denominator under one appropriately scoped assurance report.
- Consider the possibility of incorporating this common denominator into the scope of a broadly scoped SOC 2 assurance report on top of the (presumably already acquired and still valid) ISO 27001 certification. Although SOC 2 is more expensive than a regular TPM, it also holds more commercial value, which ought to be considered.

Many sectors, many customers
This scenario is characterized by complexity, given the large number of involved certifications and the large extent of overlap. It requires significant investments in terms of both time as well as financial resources. As such, the strategies in this section aim to reduce complexity and/or lower the financial burden. To maximize maturity, we suggest the following good practices:

- All certifications → Defined as minimizing audit overhead by acquiring all relevant certifications, regardless of the sector-specific nature or overlap with existing certifications.
    - Only consider certifications that are deemed relevant for the core business. A technology provider is unlikely to reap benefits from sustainability or environmental certifications, given that they stray too far from the core business.
    - Look towards comparable technology providers in the desired sector(s) to reveal relevant candidate certifications. Then, assess the potential benefits of these candidate certifications from the perspective of appealing to new customers and fostering existing customer relationships.
    - Take care not to disproportionally drive up the costs of the core product or service, due to continuous investments into expensive certifications, to the extent that one becomes too expensive for existing customers.
    - This scenario (many sectors, many customers) comes with the highest level of complexity. Certification management can take up a significant amount of time and financial resources. This situation is likely to reap the most benefits from incorporating the general optimization practices outlined below to keep the certifications affordable and manageable.

General optimization practices
The practices discussed thus far were constrained to one specific scenario. However, regardless of the number of customers, we suggest the following general optimization practices for managing standards and minimizing complexity across many sectors:

- Parallel audits → Defined as simultaneously conducting several audits of different information security standards to avoid having to endure repetitive audits.
    - Technology providers would do well to first assess all candidate certifications, taking into account the sectors in which one is currently operating as well as new sectors for potential future expansions.
    - Audit partner selection is key in order to get the most out of parallel audits. Rather than focusing on short-term cost mitigation, treat the auditor selection process the same way one would go about establishing long-term partnerships.
    - Focus on choosing auditors that are capable of auditing most (if not all) relevant standards simultaneously. In a sense, there is a bit of a lock-in principle, as it is relatively costly to change partners later on. Switching auditors at a later stage will incur a significant amount of repetitive work.

- GRC tooling → Defined as utilizing Governance, Risk & Compliance tooling for managing a technology provider's ISMS to reduce the complexity and improve the efficiency of managing certifications. When evaluating GRC tool suppliers, consider at least the following:
    - To alleviate pressure off the technology provider, consider the possibility of letting the auditors take some degree of responsibility for managing and mapping overlap among the standards.
    - Annual costs: Under €10.000 (IRM) to over €100.000 (GRC).
    - The number of supported standards: Cross-sector mapping and maintenance.
    - Implementation time: Training of employees, installation of software, relevant advisory services.
    - Compatibility with a technology provider's internal systems: Integration with applications already in-use by the technology provider.
    - Portability to and from a new GRC tool: The degree to which a technology provider is locked-in to a single supplier, potentially restricting the freedom to operate in the future.

- Diversify certifications into sub-components → Defined as diversifying one's acquired certifications by splitting them up into several smaller sub-components, each with their own separate scopes.
    - Might be worth considering in situations in which a technology provider wishes to employ several ISMSs and/or wishes to decrease the dependency on the validity of other certifications. One would do well to assess the overlap of the individual scopes of these ISMSs to figure out whether or not these justify their own separate scope.
    - Of particular interest to larger enterprises comprising of several smaller branches across several products, services or markets. This is especially relevant for international organizations that might be involved with varying degrees of regulation.

- Leverage certifications in negotiations → Defined as leveraging the reduction in audit overhead due to the acquisition of appropriate certification to assume a favorable negotiation position.
    - Show the customers that appropriate certification alleviates (at least to an extent) the need for customers to conduct extensive audits themselves. Knowing and utilizing this to one's advantage, allows a technology provider to assume a favorable position when discussing pricing options.
    - Consider the bargaining power of acquired novel certifications and/or maintaining existing certifications when renegotiating the extension of existing contracts.

Discussion on the future developments in the field
The good practices discussed above were all placed in the context of one or more scenarios. However, we would like to conclude this chapter by providing some brief discussion regarding the *future of information security certifications* in the context of a modular approach. Such a perspective is necessary, because component certification could effectively shift the focus from certification based on sector-specific regulation to certification based on competence.

It is worthwhile noting that at the time of writing this thesis, component certification has limited practical applicability, as it is essentially limited to the ISO 27001 standard with its extensions and the ETSI standards to comply with eIDAS regulation. To increase the likelihood of component certification becoming a viable method in the future, technology providers in the field are advised to participate in the discussion surrounding the development of information security standards. Technology providers seem uniquely positioned to add value to the community's efforts towards component certification. Standardization agencies, responsible for the development of standards, do not possess the same degree of practical experience and knowledge as technology providers. Yet, active participation from the field might be necessary to convey the desire for component certification (if this need is even sufficiently large to begin with) as a means of overcoming certification entry barriers.

Information security appears to be a universal need, irrespective of the sector in which one operates, but the relevant scope and desired level of information security likely vary across different industries. Component-based certification may eliminate this overlap, yet simultaneously allow for individual differences in scope and level of assurance. Regarding the development of information security standards, many sectors appear to be in the process of reinventing the wheel. As such, it is in the best interest of all parties involved to communicate with each other. Practitioners in the field should consider contributing in working groups to provide feedback and intervene early on in the development process. Although the development of standards is a never-ending process, the earlier concerns are voiced, the easier it will be to incorporate them. However, the realization of component certification is a major undertaking. Even with active participation from the field, it remains to be seen whether the industry will converge towards a modular approach. The use of regulation could be considered to overcome conflicting stakeholders' interests and facilitate the concept of a modular approach to certification.

That being said, several interview participants in this research project did not necessarily agree with the notion that conflicting stakeholder differences are a barrier to the adoption of component certification. Instead, several IT auditors and one standardization agency reported that the level of complexity is constantly rising, which becomes the driving force for a component audit. These IT auditors explained the concept of component certification from a classical view, explained in sub-section 4.2.2.5 on component certification. The IT auditors and standardization agency viewed component certification as a synchronization of tasks. They believe component certification is currently being used as an intermediary tool until the normative bodies address the increased level of complexity resulting from the constant developments in the field.

To conclude, irrespective of the perspective through which one views the role of component certification and its use, we believe that component certification is likely to become more relevant in the future in both the fields of academics and practitioners.

6 Validation

This chapter presents the empirical evaluation study, which is carried out in the last stage of the Design Science cycle [9]. Its goal is to serve as the first step towards the validation of the artifact proposed in chapter 5 (the maturity model depicted in Figure 11). As stated in chapter 3, we chose an expert-opinion-based evaluation strategy. Nine experts were interviewed regarding the *perceived ease of use, usefulness* and the *intention to use the proposed artifact in a real-world practical context*.

The participants were first provided with a briefing consisting of a written instruction to the maturity model, followed by the certification maturity model (depicted in Figure 11) itself. The full validation briefing is available to the readers of this thesis in Appendix D: Validation Briefing. If the participants had any questions after having read the instructions and studied the model, these questions were addressed to ensure all participants had a proper understanding of the model prior to starting the validation process.

Once the participants were prepared, they were given the link to fill out the treatment validation questionnaire. The questionnaire is adapted from the UTAUT validation model and consists of two phases. First, participants were asked two open questions to assess whether they recognized the concepts presented by the model and whether these concepts were located in the appropriate place. The remainder of the questionnaire were closed questions, which were measured with a 5-point Likert scale based on the following UTAUT constructs:

- Performance expectancy.
- Effort expectancy.
- Attitude towards using technology.
- Social influence.
- Facilitating conditions.
- Self-efficacy.
- Anxiety.
- Behavioral intention to use the system.
- Feedback (note: This construct was answered through open questions and not measured with a Likert scale).

The full treatment validation questionnaire is available to the readers of this thesis in Appendix C: Treatment Validation Questionnaire (UTAUT). The remainder of this chapter is structured as follows: Section 6.1 presents information about the experts who participated in the validation. Section 6.2 discusses findings related to the open questions. Section 6.3 discusses findings related to the closed questions. Section 6.4 discusses participant feedback and suggestions for improvement. Finally, section 6.5 discusses limitations of the treatment validation.

6.1 Expert Backgrounds

All participants were experts in their respective fields, but with slightly different backgrounds. Every expert possessed ample experience in the field of information security certification, either from a technical perspective or in the field of compliance. Moreover, participants from both inside and outside of Innovalor participated in the treatment validation. This section provides an overview of the experts' backgrounds. Table 5 below presents the nine experts that participated in the treatment validation, including their relevant background, work experience and areas of expertise.

Expert	Role	Description
Internal (within Innovalor)		
1	Compliance officer	20+ years of experience in the field of digital identities. Certified information systems security professional (CISSP) with a specialization in the domain of authentication solutions, eIDAS and biometrics.
2	Security officer	10+ years of experience in the field of IT security, including information security certifications. Started out as an IT consultant and developed into the role of security architect.
3	Security officer	20+ years of experience in the field of IT security. Started out as a software engineer and developed into the roles of software architect, domain architect and enterprise architect. Extended experience with information security related compliance, including certifications and GRC tooling.
4	Contract manager	4+ years of experience in the field of IT related legal work. Has work experience in the roles of privacy officer, compliance officer and contract manager, as well as experience with GRC tooling.
External (outside Innovalor)		
5	Compliance consultant	20+ years of experience, specialized in eIDAS regulation, specifically on electronic signature and trust services providers.
6	IT auditor	15+ years of experience in the field of IT auditing. Registered auditor (RA), currently operating as an independent auditor in the domain of information security certification, including ISO, ISAE, ETSI and NEN standards.
7	IT auditor	15+ years of experience in the field of IT auditing. Registered auditor (RA), CISP, CISA, QSA and 3DSQA. Has experience with audits of many standards, including ISO, ISAE, ETSI, NEN, PCI and more.
8	IT consultant	10+ years of experience, of which at least 5 years as a compliance officer. Registered auditor (RA) and predominantly works with ISAE (SOC 1 and SOC 2).
9	Standardization agency	20+ years of experience, started out as an IT consultant and developed into the domain of standardization policy. Has collaborated with other standardization bodies as well.

Table 5: Experts background.

6.2 Findings Related to the Open Questions

All nine experts unanimously recognized the certification strategies and optimization practices outlined in the maturity model. Moreover, all of them agreed that the strategies are located in the appropriate location in terms of level and order. That being said, the majority of the participants did elaborate beyond a simple yes or no by adding remarks of their own. The following answers are direct excerpts from the expert evaluation:

- *"They are ordered correctly, except maybe the optimization practice of leveraging certifications in negotiations. How does a favorable negotiation position reduce audit overhead?"*
- *"I do not think the common denominator is really a thing, you will from ISO (27001) to all the sector-specific certifications by the customer demands."*
- *"I partially recognize the constructs. The strategies assume that the organization has a choice whether or not to apply for certification. Sometimes certification is required, regardless of the maturity or organization size."*
- *"I agree with the big picture, but common denominator confuses me a little. A common denominator through a TPM is slightly different from a certification, because a TPM leverages an independent auditor who constructs an assurance report that a given organization conforms to a predefined set of controls."*

- *"I can imagine that, for larger organizations, it is possible for specific departments to have different strategies and optimization strategies, such as different certification strategies and optimization practices in one company."*
- *"I do believe this is the most logical order. The market might view 'Component certification' as a step-up to 'All certifications' in future developments. I do not believe the market is ready for such a reversal yet, as component certification is a very new concept. "*

Given the complexity and nuance of the subject matter, it is expected that not all experts agree on every aspect of the model. The experts were in agreement on the relevance and appropriateness of the overall structure of the model.

6.3 Findings Related to the Questionnaire

The results of the closed questions from the validation questionnaire are summarized in Table 6 below. All questions were answered on a 5-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree). The goal of the validation is to evaluate the experts' opinions regarding perceived *ease of use*, *usefulness* and the *intention to use the proposed artifact in a real-world practical context*. Therefore, in the following three sub-sections (sections 6.3.1, 6.3.2 and 6.3.3), we examine these three areas in detail and analyze the findings across the internal and external participants.

Criteria (N=9)	*Min. (N=9)*	*Med. (N=9)*	*Total Avg. (N=9)*	*Internal Avg. (N=4)*	*External Avg. (N=5)*
Performance Expectancy					
I would find the maturity model useful in my job	2	4	3.7	3.5	3.8
Using the maturity model enables me to accomplish tasks more quickly	2	3	3.2	3	3.4
Using the maturity model increases my productivity	2	3	3.1	3	3.2
Effort Expectancy					
My interaction with the maturity model would be clear and understandable	2	3	3.3	3.8	3
It would be easy for me to become skillful at using the maturity model	2	4	3.8	3.8	3.8
I would find the maturity model easy to use	2	4	3.6	3.8	3.4
Attitude Towards Using Technology					
Using the maturity model is a good idea	3	4	4.1	4.3	4
The maturity model makes work more interesting	2	3	3	3.3	2.8
Working with the maturity model is fun	3	3	3.2	3.3	3.2
I like working with the maturity model	2	3	3.2	3.5	3
Social Influence					
People who influence my behavior think that I should use the maturity model	1	3	2.7	3.5	2
People who are important to me think that I should use the maturity model	1	3	2.6	3.3	2
Facilitating Conditions					
I have the resources necessary to use the maturity model	2	4	3.6	4.5	2.8
I have the knowledge necessary to use the maturity model	3	4	4.1	4.5	3.8
The maturity model is not compatible with other systems I use.	1	2	2.3	1.8	2.8
Self-Efficacy					
If there was no one around to tell me what to do as I go.	2	4	3.7	4	3.4
If I could call someone for help if I got stuck	1	3	3.1	3.5	2.8
If I had a lot of time to complete the job for which the maturity model was provided	1	3	3.2	3.5	3
If I had just the built-in help facility for assistance	3	3	3.4	3.8	3.2
Anxiety					
I feel apprehensive about using the maturity model	1	3	2.6	3	2.2
The maturity model is somewhat intimidating to me	1	1	1.8	2	1.6
Behavioral Intention to Use the System					
I intend to use the maturity model in the next 6 months	2	3	3.1	3.8	2.6

Table 6: Validation questionnaire results.

Table 6 summarizes the results of all nine experts. The rows display the UTAUT questionnaire constructs with their corresponding questions, while the columns summarize simple descriptive statistics of the questionnaire results. From left to right, the descriptive statistics consist of the minimum (Min.), median (Med.) and average (Avg.) values. Findings highlighted in green indicate a strong positive deviation, at least one point away from neutral (three). Conversely, findings highlighted in orange indicate a strong negative deviation, at least one point away from neutral (three).

The first three columns contain the cumulative data for all nine participants. However, four out of the nine experts originated from Innovalor (internal experts), while the remaining five experts originated outside of Innovalor (external experts). As such, we believe it is sensible to distinguish between these two groups of internal and external participants. Distinguishing between internal and external stakeholder groups shows potential discrepancies or stakeholder bias between experts from both groups. The internal group findings (average results) are displayed in the fourth column and the external group findings are displayed in the fifth column. Neither of the groups were particularly homogenous in terms of backgrounds (as shown in section 6.1 on expert background), but the external group did contain a slightly more diverse range of backgrounds.

6.3.1 Perceived Ease of Use

When analyzing the findings related to *perceived ease of use*, the findings related to **Effort Expectancy, Attitude Towards Using the Technology, Anxiety** and **Self-Efficacy** are relevant (see Table 6).

Eight out of the nine participants had no trouble understanding and utilizing the model during the validation interviews. One participant asked a few additional questions about how to interpret and read the model. Upon answering the questions, the participant experienced no further difficulty in completing the questionnaire. Overall, participant feedback relating to *perceived ease of use* was considered positive, with only slight differences between the two expert groups. However, the data appears inconclusive on three out of the four questions regarding **Attitude Towards Using the Technology**, where the participants response appears neutral (averaging around three). These neutral findings possibly indicate that these questions may have been less relevant or that the wording of these questions might have been insufficiently clear to the participants.

6.3.2 Perceived Usefulness

When analyzing the findings related to *perceived usefulness*, the findings related to **Performance Expectancy, Attitude Towards Using the Technology, Social Influence** are relevant (see Table 6).

Overall, participants perceived the model to be useful, but one particular finding stands out. Irrespective of stakeholder group, participants unanimously scored the question *"Using the maturity model is a good idea"* at an average of at least four on the Likert scale. In addition, the findings on **Social Influence** warrant some additional discussion. Compared to the internal experts, the external experts seemed to be less affected by social influences of their peers. We attribute this discrepancy to the fact that the internal experts had peers to discuss the model with, which the external experts lacked.

6.3.3 Intention to Use in Practice

When analyzing the findings related to *intention to use in practice*, the findings related to **Behavioral Intention to Use the System** are relevant (see Table 6).

Only one question in the questionnaire was related to *intention to use in practice*, providing limited data for analysis. The internal experts showed a higher intention to use the model in practice, whereas the external participants appeared to be less interested in applying the model in their own operations. However, it is important to consider that the model was designed to be used by technology providers. The external stakeholder group did not contain any technology providers. A more extensive validation with a larger sample size could provide better insight into this matter and rule out any potential bias.

6.4 Participant Feedback & Improvement Suggestions

Three out of the nine participants reported one or more shortcomings of the model. The reported shortcomings below are direct excerpts from the evaluation and are summarized as follows:

- *"I think the model correctly represents reality (i.e. the scenarios outlined on the horizontal axis) and provides good guidance on certification strategies. However, the arrows in between the scenarios indicate a growing path. I believe that this growing path does not fit for all companies and think it is unnecessary for this research."*
- *"The model is still theoretical and may be too abstract. It will not add value when explaining to customers why we do not have certain certifications."*
- *"The usability of the model in larger organizations with decentralized approaches and strategies."*

We take this opportunity to reflect on the reported shortcomings. First, regarding the growing path indicated by the arrows, we agree with the expert that not necessarily every organization will follow the linear path outlined by the arrows. The growing path denoted by arrows is merely a suggestion for increasing the level of maturity (if there is a need for doing so depending on the scenario), but we do not exclude the possibility that one can deviate from the path outlined in the model. However, while not every organization will follow the linear path outlined in the model, we do believe that the majority of the technology providers will resonate with the outlined growth path. The model is intended to aid in the decision making process, but one should never carelessly rely on a model to produce a linear one-size-fits-all solution.

Second, regarding the inability to leverage the model in order to convince customers why certain certifications are unnecessary. We believe that this is a valid point and indeed a shortcoming of the model, although we would like to mention that the model was not designed to be able to convince customers that one does not require a particular additional certification in the first place. Third, we agree that the usability concerns in larger organizations with decentralized approaches and strategies is a valid concern. Given the limitations of the validation of this research project, we cannot conclude with certainty whether or not the model is applicable in larger technology providers.

Despite these shortcomings, the experts thought that the maturity model is still usable. Moving on, besides the aforementioned shortcomings, four out of the nine participants reported suggestions for improvement. Once again, the following suggestions for improvement are direct excerpts from the evaluation:

- *"Although this is slightly out of the scope of this research, you could extend the model by providing a tree-branch model for baseline certifications that coincide with the maturity levels, though it would be difficult to find baseline certifications that are internationally recognized (e.g. NEN 7510 is not internationally recognized despite its similarity to ISO 27001)."*
- *"Perhaps you can clarify that optimizing the level of maturity is not a goal in and of itself, but rather a consequence of the context in which a technology provider operates. It also think you could clarify that the optimization practices apply to all scenarios on the horizontal axis."*
- *"I would Recommend GRC tooling earlier on, as soon as one is aware that multiple certifications are required. In addition, starting with ISO 27001 or NEN 7510 (depending on the sector) is always a good idea.*
- *"Make sure to focus on risks. Clarify that certifications do not take away one's responsibility to keep doing assessments."*

We believe that all of these are valid suggestions for improvement. In particular, the tree-branch suggestion for baseline certifications selections could be interesting and may be relevant for future research that comparatively analyzes different standards and frameworks. To conclude, this initial expert evaluation with nine participants moderately supports real-world applicability of the evaluated maturity model in the context of technology providers.

6.5 Limitations

This evaluation study has some limitations. First, it includes only nine practitioners. We consider this as a threat to generalizability of the findings and therefore we acknowledge that it would have been much more beneficial if we had included more stakeholders. However, our participants are selected because of their typicality, level of engagement in security certification, expertise in the field and also because they share some commonalities, specifically: (1) Profound knowledge of Innovalor's organization, (2) expert knowledge of the business sector of technology providers and (3) expert knowledge of security audit processes and standards.

Following Wieringa [9] and Seddon & Scheepers [46], we think that it might well be possible that the perceptions of these nine experts would be similar to the perceptions of other specialists who share the same expert level of familiarity with the security certification context. This is possible because, as per the methodological discussion of Seddon & Scheepers [46], similar work contexts may create similar organizational mechanisms which, in turn, could lead to similar observations of working in the field. Of course, it will be beneficial to replicate our evaluation with more participants, which forms a line of research for the future.

Second, the author of this thesis is aware of the possible threat due to researcher's bias. This is common for any qualitative evaluation study of design science artifacts. We think, however, that this threat is minimal, because the researcher collected the experts' perceptions by using a predefined questionnaire and had access to the experts to ask clarification questions in a follow-up calls. Finally, the author has shown his analysis to the Innovalor practitioner who read this thesis completely. The review of this practitioner did not reveal any misinterpreted information regarding the conclusions of the evaluation.

Finally, the limited sample size for the validation study could potentially explain the lack of pronounced differences when interpreting the questionnaire data. Given the small sample size and qualitative nature of the subject matter, no statistical testing was performed. Instead, we relied on answers to the open questions and averages of the questionnaire items. However, the majority of the questionnaire responses yielded an average result in relative close proximity to neutral (a value of 3 on a 5-point Likert scale). This could be due to an insufficiently large sample size, resulting in an inability to generate strong findings. However, it could also indicate that the wording of the questions was insufficiently clear to the participants of the validation study, thus leaving them inclined to respond in a neutral way. We speculate that this might have been due to the fact that TAM and UTAUT models were originally intended to be used for predicting user acceptance for a proposed information system or information technology. However, this research project applied UTAUT to predict the success of a certification maturity model, instead of an information system. We consider this a potential threat to the validity of the validation process and future research in a similar setting could opt to reconsider alternative validation models.

7 Discussion on the Results and on Validity Threats

This chapter discusses the results presented by this research. Section 7.1 reflects on the results of the problem investigation and treatment design phases. Section 7.2 discusses the limitations and potential threats to the validity of this research.

7.1 Discussion

This section discusses the results of the interviews conducted for the problem investigation and treatment design phases in further detail. We start by briefly going over the two separate phases, followed by a detailed discussion on relevant interview responses from the experts who participated in the treatment design interviews.

First, we briefly address the problem investigation phase. The problem investigation interviews sample size was rather small (three participants), because Innovalor is an SME with only a few employees who are actively involved in the field of compliance and certifications. However, the three individual participants possessed different backgrounds and their responses converged, resulting in relatively unanimous interview findings.

In contrast, the treatment design interviews warrant additional discussion. What stands out the most from these interviews is the variability in responses, both within a given stakeholder type and across the different stakeholder types. In particular, the IT auditors and standardization agencies yielded different responses, whereas the technology providers appeared to be more on the same line of reasoning with similar experiences. In the context of qualitative interviews on a complex subject, such as information security certification, higher degrees of variability among participants is to be expected. Even within the same group of stakeholders, the experts who participated are not part of the same organization; they might operate in slightly different circumstances or they might have different experiences with the same topic.

In some cases, these differences of opinions could be explained by a lack of nuance leading to seemingly conflicting responses. However, occasionally, the participants upheld contradictory opinions altogether. An example of these differences occurred when participants were asked about the differences in the level of provided assurance when comparing a SOC 2 assurance report to an ISO 27001 certification. Both of these are considered comparable, given the fact that both of these constitute as organization-wide general information security certifications (although SOC 2 is technically considered to be an assurance report, not a certification). As an assurance report, SOC 2 permits a greater degree of freedom when determining the scope and relevant controls, providing more assurance with respect to operational effectiveness of the security controls. Conversely, ISO 27001 is a certification rather than an assurance report. Therefore, the organization is permitted a lesser degree of freedom when considering the relevant scope and set of controls. Yet, it provides less assurance as the focus is mostly on checking whether the internal control measures are designed/documented properly and whether they are implemented (*opzet en bestaan* in Dutch), but to a lesser degree whether they are working effectively (*werking* in Dutch). While it is certainly true that ISO 27001 incorporates a statement of applicability, it is still considered to be more predefined than assurance reports.

The interview participants were asked which of these (ISO 27001 or SOC 2) provided better assurance in checking whether the security controls are working effectively. Some reported that ISO 27001 provides more assurance in this aspect, others said that SOC 2 provides superior assurance, while the remainder argued that it depends on the way one defines assurance in the context of assessing whether controls are working effectively. As such, the limited observational data appears inconclusive, which indicates the complexity of the topic and need for additional nuance.

That being said, based on the results of the treatment validation of the certification maturity model (presented in chapter 6), we believe to have successfully incorporated the different perspectives into a holistic model. The remainder of the discussion section elaborates on the role of component certification and why it was modeled as a potential future development, separate from the remaining certification strategies and optimization practices.

Regarding component certification, all interview participants (irrespective of their background) agreed that, in theory, component certification would be desirable. However, the opinions were divided regarding its feasibility. The IT auditors reported a reluctance in trusting the work of another auditor,

because they are responsible for the to-be-certified scope, even if that same scope contains areas that have already been certified by other auditors. The auditors expressed a fear of being held accountable for potential errors made by their peers and as such, would rather repeat tasks that fall under their scope, but were already addressed in prior audits. Moreover, if component certifications were to be applied on a wide scale, both the number of standards and the size of the audits would be diminished, which could negatively affect an auditor's source of income and profit margins. Most IT auditors did not dismiss the concept a modular approach right away, but stated they are unlikely to take initiative towards realizing a modular approach.

The standardization bodies all acknowledged the seriousness of the concerns experienced by the technology providers and agreed that it might have been better if the certification process had been designed based on a modular approach from the beginning. However, the participants' opinions diverged on the feasibility of future developments towards a commonly agreed upon information security baseline, supplemented by specific process and/or product certifications. Some mentioned that they do not expect any fruitful outcomes towards component certification in the next 50 years and that standardization bodies merely develop standards based on demand from the market. They added that one should not depend on a standardization body to take initiative towards the realization of component certification, because they follow demand rather than being on the forefront of groundbreaking developments.

However, other standardization bodies spoke enthusiastically about component certification as a promising solution to the ever-growing demands for individualized certification schemes resulting from the rapid increase in outsourcing. These standardization bodies mentioned that they are actively pursuing these developments in the context of European harmonization, but that it is still unclear how several factors such as regulation (national and sector-specific differences), cooperation of standardization bodies and cooperation of competent auditing agencies will shape the developments. In particular, regarding cooperation among standardization agencies, the participants touched on some of the practical hurdles regarding the collaboration of standardization agencies worldwide and stated that it is still unclear to them whether a modular approach will even reach widespread adoption at all. It is clear that not all standardization bodies are on the same page, with some proactively taking on a leading role to steer the market in a certain direction, while others primarily react to market demand.

To summarize, it has become evident that component certification has been a topic of discussion for at least over a decade, but most efforts towards its realization have not yet led to fruitful outcomes, most likely due to the complexity of the situation and stakeholder-specific conflicting interests. However, organizations should not let compliance lead to complacency. An overreliance on certifications poses a risk for organizations to rely on certifications as a false sense of security, which we have also noted in the literature review for this research project [3]. It is essential that technology providers continue to conduct their own risk analyses.

7.2 Reflections on Validity Threats

This section is the author's reflection on the potential threats to the validity in this research in order to ensure appropriate interpretation of the results and promote transparency. For this reflection, the methodological source of Wieringa [9] is used as a guideline to frame the discussion.

First, the background chapter of this thesis included a systematic literature review in which we summarized findings from the literature regarding the value of information security certification. However, given the scope of this research, we did not assess the individual type of methods that were used in the literature (such as use cases, empirical experiments and so on) to make these claims about information security certification. Although we do not believe this detracts from the usability of the literature findings for this thesis, it is nonetheless a potential shortcoming of the literature review and may be of interest to academics looking to perform research on this topic in the future.

Regarding the interviews, it is important to point out that the sample size for the problem investigation interviews is rather small **(3 participants)**. However, one should consider the fact that Innovalor is still a relatively young startup and small company in terms of number of employees. Roughly 35 employees are active as of the writing of this thesis, classifying them as an SME. As such, not many employees within the organization are actively involved in information security certification. For this reason, three experts with varying backgrounds within Innovalor were interviewed in order to get a multidisciplinary perspective on the problems. The goal of the interviews was to identify practical challenges regarding

current information security certification practices. This helps with the understanding of what causes these challenges and why it is desirable to treat them. Moreover, these interviews may reveal existing treatments or point the research towards an initial treatment design. The three experts' responses were relatively unanimous, suggesting an acceptable degree of saturation. Ideally, the problem investigation sample size would have been larger and should be considered as a minor threat to the validity of this research.

The sample size of the interviews conducted for the treatment design **(18 participants)** is larger compared to the problem investigation phase **(3 participants)**, because the treatment design calls for the inclusion of a wider range of stakeholders. Compared to quantitative interviews, the sample size of qualitative interviews can be lower, because the data frequency occurrences are less important and qualitative research is relatively labor intensive. Although saturation was not reached across all aspects of the treatment design interviews, the cumulative sample size for this research **(21 participants)** is in line with the qualitative interview recommendations regarding phenomenological studies, as well as the general qualitative interview sample size guidelines (as discussed in chapter 3). Due to conflicts of interest between stakeholder types, not every topic reached a consensus among the participants (as described in the discussion in the last section). However, we nonetheless generated useful findings. Because of the large stakeholder differences and occasional contradictory responses among the participants, the concept of saturation was not fully achieved. However, we argue that the sample size was sufficiently large to generate useful findings. With every additional interview, less novel information was gained and more repetitive responses were given. As such, although saturation was not fully achieved, the increasingly marginalized benefits of additional interviews and the inability to extend the duration of the research beyond the scope of 6 months resulted in a cutoff point of **21 participants.** Moreover, intended to interview five different GRC tool suppliers to be able to provide a comparative analysis regarding GRC tooling's capabilities and limits. However, only one supplier agreed to participate in the study. These limitations ought to be considered when interpreting the interview findings associated with GRC tooling.

Overall, this thesis should be considered as exploratory research. We approached the research problem from a high-level perspective and only dabbled in technical aspects. Based on our interpretation of the literature and interviews, we depicted a high-level overview of the certification landscape by comparing several information security standards as part of the problem investigation (depicted in Figure 7). Proper comparative research on the degree of overlap between security standards is warranted to validate and/or improve this analysis in further detail. In particular, detailed mapping of information security standards could prove useful in gaining insight into the degree of overlap and for realizing future developments.

Regarding the maturity model that we presented in chapter 5 and the strategy selection framework introduced in section 4.2.4, it remains possible that this initial model is still incomplete. Considering the relatively narrow scope of this research and a cumulative interview sample size of **21 participants**, it is not beyond any reasonable stretch of the imagination that there are candidate strategies which were not discovered during the execution of this research. This potential shortcoming poses as a threat to the validity of this research and ought to be considered as such. Future research grounded on more extensive empirical data might expand or revise the model introduced in this thesis.

Continuing along the line of possible threats to validity, serious efforts were made to stay as objective as possible. However, this research was sponsored by Innovalor, which means that it is not inconceivable that the author of this paper may be exposed to some degree of unconscious bias towards developments that disproportionately favor technology providers (such as Innovalor). Although the research was performed in cooperation with Innovalor, the practical supervisor did not influence the direction of the research.

Regarding researcher bias, we would like to take this opportunity to state that the author of this research has limited experience and knowledge in the field of information security certification and IT auditing. The only prior research conducted by the author of this research is a systematic literature review on the topic of information security certification and IT auditing [3], which was done in preparation for this thesis and has been incorporated into the background section of this research. In addition, the academic supervisors do not have any prior published work in the field of information security certification. Therefore, we believe that no subjective bias is passed into this thesis due to possible researcher's

knowledge of authors of included papers. As such, there was no explicit bias from the industry, the academic supervisor or myself.

Finally, an interesting question in design science research is about the extent to which the proposed artifact, the proposed maturity model, could be used beyond the context for which it was originally created. To have a substantiated claim in regard to this, more empirical evaluation research is required in other technology providers' organizations. However, following Wieringa's reasoning [9] about generalizability across similar context, we could possibly assume that the proposed maturity model might well be suitable to contexts similar to the one of Innovalor. As Wieringa (2014) suggests, organizations operating in the same business environment, providing similar services, sharing similar goals, similar initiatives and similar needs might well find useful to consider for implementation of artifacts that were created in other similar but different organizations. If an artifact created for one organization (i.e. Innovalor) is perceived as useful in its original context, this artefact could possibly be perceived as useful in other similar organizations that share contextual similarities with Innovalor.

Related to the above paragraph, we add a personal reflection on the cultural context in which this research happened. One may say that Innovalor operates in Northwest Europe. Therefore, when generalizing the use of our maturity model to other companies, we could expect similar observations to be observable in similar companies in other Nordic countries that have a comparable culture and attitude towards security (e.g. Germany, Denmark or Sweden). However, would the model be applicable to countries in other continents, such as in Japan? The author decided to add a reflection on this, because he was on an educational stay in this Asian country and got exposed to experiencing a culture vastly different from the Netherlands in any way imaginable.

In the western world, our cultures can be characterized as individualistic societies. Culturally speaking, we often regard the rights of the individual above the purpose of the society as a whole. Contrary to these western values, the Japanese society can be characterized as a collectivistic one, where one's contribution towards society is often considered to be more important than the rights of an individual. The Japanese culture is centered around the concepts of respecting those around you (even strangers), avoiding conflict and trying one's hardest to provide value to society as a whole. In addition, one could describe their society as more bureaucratic in nature, heavily structured around rules and procedures.

Given the bureaucratic tendencies and presence of large IT advisory & auditing corporations (including but not limited to Deloitte, PwC, EY and KPMG) in Japan, we speculate that the certification maturity model introduced in this research may (at least in part) be applicable to the Japanese market as well. Assurance by an independent party that an organization conforms to a given security standard is likely to be desirable for the sake of compliance with the many rules and regulations. However, one ought to consider that business etiquette and working culture in Japan vastly differ from the west. Moreover, the standards discussed in the context of this research project are relevant for the Dutch and European market, but not necessarily for the Japanese market. Therefore, we speculate that the core principles of the model presented in this thesis likely hold true in the Japanese context as well, but that the specific recommendations and good practices likely require adjustments in order to bridge the continental gaps between Asia (specifically Japan) and Europe.

8 Conclusions

This master's thesis has investigated six research questions within a research project aiming at the design of a maturity model for treating the challenges associated with information security certification by supporting technology providers in choosing an effective information security certification strategy.

This chapter briefly summarizes the findings per research question and provides closing thoughts on implications for practice and for future research. Section 8.1 lists the novel contributions of this research. Section 8.2 summarizes our most important conclusions following the order of the six research questions. Finally, section 8.3 presents the implications for practitioners in the field, implications for academics and suggestions for future research.

8.1 Contributions

This research project made the following contributions, summarized as follows:

- We derived a high-level conceptual model of the certification process based on a systematic literature review (see Figure 3, section 2.1). This model resulted out of the research efforts, in preparation for this thesis and is part of the background chapter of this thesis [3].
- We provide a conceptualization of the certification landscape from Innovalor's perspective based on our interpretation of the results of the problem investigation interviews, resulting in a high-level comparison of several certifications (depicted in Figure 7, section 4.1.2).
- We introduced the notion of a *technology provider certification lifecycle*, showing the variability in certification needs as a technology provider progresses through four possible scenarios (depicted in Figure 8, section 4.2.1).
- We constructed a certification strategies selection framework, which maps the five certification strategies and four general optimization practices onto the scenarios from the certification lifecycle (depicted in Figure 9, section 4.2.4).
- We designed the ultimate artifact of this research, namely the certification maturity model (depicted in Figure 11, section 5.2). This was achieved by combining all of the previous findings and integrating the contributions listed in the previous bullet points.

8.2 Answers to the Research Questions

This research has investigated six research questions. This section briefly summarizes the findings of the six research questions.

RQ1: *What challenges do technology providers face regarding information security certifications?*
According to the systematic literature review that we conducted in preparation for this thesis [3], the most pronounced challenges associated with information security certifications in general are:

- Genericity of frameworks.
- Increasing complexity of the IT security audit landscape.
- Significant financial costs associated to certification.
- Dependence on individual auditor competence.

Furthermore, in the problem statement and problem investigation sections, we presented the following additional practical challenges in the context of technology providers:

- Deciding if and when to start with certifications.
- Selection of appropriate certification(s).
- Selection of appropriate auditing partner(s).
- Managing overlap between certifications.
- The lack of cross-sector applicability of certifications.
- Integration between different certification schemes is complex and error prone.
- Existing certification schemes are not catered to the use of widespread outsourcing and sub-contracting.

RQ2: *What are the current common practices of information security certification?*
Based on the occurrences within the academic literature, a distinction was made between general information security frameworks, financial sector-specific frameworks and healthcare sector-specific frameworks. The most commonly adopted frameworks and standards are [3]:

- General information security certification: ISO/IEC 27001, COBIT, ITIL, Common Criteria and the NIST/FISMA risk management framework.
- Financial sector-specific certification: PCI DSS and SOC 2. To clarify, SOC 2 is applicable in many sectors. It was not designed specifically for the financial sector, nor is it legally required by regulation in Europe. However, SOC 2 has adopted the role of becoming the financial sector industry standard.
- Healthcare sector-specific certification: HIPAA Security Rule (United States) and NEN 7510 (the Netherlands).

Subsequently, in the problem investigation phase we analyzed the adoption of certifications among 17 technology providers operating in Europe and concluded that ISO 27001 is the most widely adopted standard (depicted in Table 3). Besides that, the certification landscape appears fragmented, with a significant number of different standards seeing adoption in practice.

Lastly, as we have shown in the systematic literature review [3], the value of information security certification largely depends on the success of IT audits. Therefore, we argue that IT audit success factors ought to be considered as common practices in the context of security certification. The most prominent success factors come from Merhout and Havelka's [12] IT audit success factor model, who defined the following eight factors:

- Audit process.
- Social IT auditor competence.
- Technical IT auditor competence.
- Audit Team.
- Client-controlled organizational factors.
- IT audit-controlled organizational factors.
- Enterprise & organizational environment.
- Target process & system.

RQ3: *What strategies exist for satisfying information security demands through certifications?*
The research put forward the following five information security certification strategies:

- **No certification by an independent third party**: Refrain from acquiring certification by an independent third party and accept additional audit overhead.
- **Sector-specific certification**: Adopt the most desirable sector-specific certification based on customer demands.
- **Common Denominator:** Certify a common denominator of sector-specific security controls, ideally auditing once to comply with many standards.
- **All certifications:** Minimize audit overhead by acquiring all relevant certifications (as per customer demand) to satisfy the customers' security demands, regardless of the sector-specific nature or overlap with existing certifications.
- **Component certification:** A general organization-wide security baseline supplemented by specific in-depth product and/or process certification(s).

Besides that, we defined four general optimization practices, which are separate from the abovementioned strategies. These optimization practices can be utilized in conjunction with any of the previously mentioned strategies, acting as supplementary tools to promote efficiency and mitigate complexity. The following four optimization practices were defined:

- **Parallel audits:** Conduct several audits of different information security standards to avoid having to endure repetitive audits.
- **GRC tooling:** Utilize Governance, Risk & Compliance tooling to reduce the complexity and improve the efficiency of managing certifications.

- **Leverage certifications in negotiations:** Leverage the reduction in audit overhead due to the acquisition of appropriate certification to assume a favorable negotiation position.
- **Diversify certifications into sub-components:** Diversification of acquired certifications by splitting them up into several smaller sub-components with their own separate scopes.

RQ4: *What are the advantages and disadvantages of the different strategies?*
The five certification strategies and four general optimization practices with their corresponding advantages and disadvantages were listed in section 4.2.4.2 of this thesis (see Table 4). Our reasoning on the advantages and the disadvantages is provided in terms of aspects such as internal and external auditing costs, flexibility, cross-sector applicability, references to established standards, compliance requirements and requirements for migration of processes, among others. It is important to note that each of our suggested strategies "scores" differently in regard to these aspects. Therefore, each company first needs to know which of the aspects are important to them and only then look at the advantages and the disadvantages.

RQ5: *What are the factors that influence strategy selection?*
This research has shown the context dependency of appropriate certification strategy selection. In section 4.2.1, we introduced the concept of a technology provider certification lifecycle, which is portrayed in Figure 8. From that, the primary takeaway appears to be that certification needs are *situational,* meaning that the context in which a given technology provider operates plays a crucial part in the selection of an appropriate certification strategy. We introduced four novel situational factors (first depicted in Figure 8) and defined them as the following four scenarios:

- **Few sectors, few customers:** The scenario for startups with limited resources that have not yet been able to generate many customers.
- **Few sectors, many customers:** The scenario for niche SMEs that have grown out of the startup phase by generating more customers, but are still restricted to operating in a small number of sectors.
- **Many sectors, few customers:** The scenario for SMEs that are expanding and branching out into new sectors, exposing themselves to sector-specific certification entry-barriers or significant audit overhead.
- **Many sectors, many customers:** The scenario for larger organizations that have expanded their services across sectors and accumulated a relatively large pool of customers, exposing themselves to higher levels of complexity regarding the management of certifications.

Besides the abovementioned scenarios, the following contextual factors emerged from the interviews:
- Financial and human resources.
- Desired degree of flexibility.
- Quantity of customers.
- Customer homogeneity.
- Relevant regulation.
- Sector specificity of a given standard.

RQ6: *What is the applicability of the proposed artifact?*
- **RQ6.1:** *To what extent is the proposed artifact useful to practitioners in the field?*
    - The practitioners from the field showed that the evaluated artifact (certification maturity model) sufficiently and accurately represents reality. In addition, the artifact was perceived to be both useful and easy to use. However, no technology provider from the field participated in the evaluation study, thus we cannot give a conclusive answer regarding applicability of the artifact to technology providers in the field.

- **RQ6.2:** *To what extent is the proposed artifact usable by Innovalor?*
    - The data of the expert evaluation within Innovalor indicates that the participants responded positively regarding the perceived ease of use and perceived usability of the artifact. We conclude that the certification maturity model helps Innovalor by providing guidance when selecting an appropriate information security certification strategy and facilitates the construction of a certification roadmap.

8.3 Implications & Future Research

This section presents the implications of this research. It addresses generalizability, practical recommendations for practitioners and finally, recommendations for academic researchers looking to conduct research in the future and implications for university teaching.

First, regarding generalizability, this research was conducted in the context of technology providers responsible for the execution of one or more generic outsourced sub-processes for their customers across multiple sectors. These providers struggle tremendously with the fact that traditional certification schemes are not catered to the widespread utilization of outsourcing specific processes to third parties. The certification maturity model presented in this research provides added value through supporting technology providers in developing an information security certification strategy based on their context and ambitions, which did not exist prior to this research project.

We believe that the findings of this research are likely to be generalizable to the extent of technology providers who are responsible for the delivery of generic outsourced sub-processes from their customers. However, we speculate that particular attention ought to be drawn to the fact that traditional certification schemes are not catered to the widespread utilization of outsourcing. Further research is required to assess applicability of the findings across a wider scope, such as certifications in general (rather than just in the domain of information security) or beyond the scope of technology providers (such as outsourcing of processes in a broader context).

Second, for practitioners in the field, the practical takeaway from this research is that the information security certification landscape remains *fragmented*. A large number of information security standards have been developed and novel standards continue to emerge. Some of these standards directly compete against each other, while others appear to be complementary. Given this volatility, we believe that the best bet for organizations is to consider participating in the discussion surrounding information security standards. Working groups on the development of new standards or maintenance of existing ones, are likely to be an invaluable channel through which practitioners from the field can share their experiences and directly provide feedback to standardization bodies.

Regarding the artifact of this research, we believe application of the maturity model is likely to aid in the decision-making process for technology providers that are considering appropriate options for pursuing information security certifications. The maturity model designed to be used in a prescriptive manner and may facilitate the construction of a development roadmap by indicating how an organization can improve the maturity of their information security certifications to positively affect the value of the business.

Third, this paper has some implications for academic researchers. This research is a proposal with an initial validation (in terms of the design science exercise [9]). Our evaluation study indicates that the maturity model shows promise, but is still an initial model in itself. Therefore, more empirical evaluation studies on its application in real-world contexts are needed and, in turn, form a line for future research. Based on the findings in this thesis, the following topics may be of interest to academic researchers looking to conduct future research:

- A more elaborate evaluation of the certification maturity model proposed in this research. The initial validation's limited sample size and domain-specific usability could be expanded upon. An evaluation on larger scale could lead to stronger findings and reveal challenges related to certifications from a wider range of technology providers.
- Exploring the possibility of expanding the model to promote generalizability across a broader scope. In particular, the following areas may be of interest:
    - Applicability outside of Europe, e.g. in Japanese or American context.
    - Applicability beyond the scope of technology providers, such as outsourcing in general. In particular, we hypothesize that outsourcing of generic sub processes in general could be considered as a candidate scope in future research.
    - Applicability to certifications in a broader context (outside the domain of information security).
- A comparative analysis on the degree of overlap among different information security standards through extensive mapping of the standards' underlying security controls.
- Further research into the developments concerning the concept of a modular approach to certification, which we described as component certification in this research. In particular,

monitoring and evaluating current and future developments concerning ETSI standards is advised, given their tendency to take a leading role in the facilitation of modular certification.

- The related work included a systematic literature review, however did not assess the individual type of methods that were used to make these claims about certification. Future literature reviews could expand on our review by taking these research methods into account.

Finally, in the context of university programs, this work can be utilized by cybersecurity teachers who educate students in courses dealing with organizational aspects of security. If a teacher wants to educate students in the field of IT auditing and the complexity of information security certification, this master's thesis provides a real-world case (Innovalor) and contextually rich information on the problems that technology providers (such as Innovalor) face and the possible remedies to these problems. We have shown that certification needs vary and are highly context-specific, indicating that there is no one-size-fits-all approach. Professional judgement on a case-by-case basis from all parties involved is crucial in the rapidly evolving field of information security certifications and IT auditing.

9 References

[1] M. Majdalawieh and I. Zaghloul, “Paradigm shift in information systems auditing,” *Eletronic Libr.*, vol. 34, no. 1, pp. 1–5, 2017.

[2] S. Ali, R. Ashrafi, and S. Al Busaidi, “Application integration and audit control in orgnisational merger: Case of Oman,” *J. Theor. Appl. Inf. Technol.*, vol. 79, no. 3, pp. 514–527, 2015.

[3] M. Hulshof, “The value of information security certification : A systematic literature review,” 2021.

[4] T. Rosário, R. Pereira, and M. M. Da Silva, “Formalization of the IT audit management process,” *Proc. 2012 IEEE 16th Int. Enterp. Distrib. Object Comput. Conf. Work. EDOCW 2012*, pp. 1–10, 2012.

[5] B. Hulsebosch and A. van Velzen, “Inventarisatie en classificatie van standaarden voor cybersecurity,” InnoValor, 2015.

[6] B. R. Aditya, R. Ferdiana, and P. I. Santosa, “Toward Modern IT Audit- Current Issues and Literature Review,” *Proc. - 2018 4th Int. Conf. Sci. Technol. ICST 2018*, vol. 1, pp. 1–6, 2018.

[7] B. R. Aditya, R. Hartanto, and L. E. Nugroho, “The Role of IT Audit in the Era of Digital Transformation,” *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 407, no. 1, 2018.

[8] “REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.”

[9] R. J. Wieringa, *Design science methodology: For information systems and software engineering*. 2014.

[10] V. I. Daskalova and M. A. Heldeweg, “Challenges for Responsible Certification in Institutional Context: The Case of Competition Law Enforcement in Markets with Certification,” Springer, Cham, 2019, p. 31.

[11] H. Salminen, “Success factors and pitfalls in security certifications,” in *European Conference on Information Warfare and Security, ECCWS*, 2019, vol. 2019-July, pp. 811–818.

[12] J. W. Merhout and D. Havelka, “Information Technology Auditing: A Value-Added IT Governance Partnership between IT Management and Audit,” *Commun. Assoc. Inf. Syst.*, vol. 23, pp. 463–482, 2008.

[13] C. Di Giulio, R. Sprabery, C. Kamhoua, K. Kwiat, R. H. Campbell, and M. N. Bashir, “Cloud Standards in Comparison: Are New Security Frameworks Improving Cloud Security?,” in *IEEE International Conference on Cloud Computing, CLOUD*, 2017, vol. 2017-June, pp. 50–57.

[14] C. Gikas, “A general comparison of FISMA, HIPAA, ISO 27000 and PCI-DSS Standards,” *Inf. Secur. J.*, vol. 19, no. 3, pp. 132–141, 2010.

[15] A. Fiedler, N. Dunham, C. Thiel, and I. Barreira, “Towards global acceptance of eIDAS audits About ENISA Contributors Acknowledgements,” 2018.

[16] I. Barreira *et al.*, “Analysis of standards related to Trust Service Providers - Mapping of requirements of eIDAS to existing standards,” 2016.

[17] ENISA, “Assessment of Standards related to eIDAS Recommendations to support the technical implementation of the eIDAS Regulation,” 2018.

[18] KNMG, “Gedragscode Elektronische Gegevensuitwisseling in de Zorg (EGiZ),” 2019.

[19] ETSI, “ETSI 119 461- Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects,” vol. 1, pp. 1–24, 2018.

[20] Norea, “HANDREIKING ENSIA voor IT-auditors (RE’s) Eénduidige Normatiek Single Information Audit voor gemeenten,” 2017.

[21] J. King, N., Horrocks, C., Brooks, *Interviews in Qualitative Research*. 2019.

[22] R. E. Roberts, “Qualitative interview questions: Guidance for novice researchers,” *Qualitative Report*, vol. 25, no. 9. pp. 3185–3203, 2020.

[23] J. Saldaña, “The Coding Manual for Qualitative Researchers (2nd edition),” *Qual. Res. Organ. Manag. An Int. J.*, vol. 12, no. 2, pp. 169–170, 2017.

[24] A. Osterwalder, “The Value Proposition Canvas,” *Career Anal. Des.*, p. 1.

[25] M. Mason, “Sample Size Saturation in PhD Studies Using Qualitative Interviews,” pp. 1–14, 2010.

[26] K. C. Charmaz, “Constructing grounded theory. A practical guide through qualitative analysis,” *Int. J. Qual. Stud. Health Well-being*, vol. 1, no. 3, 2006.

[27] G. Guest, A. Bunce, and L. Johnson, “How Many Interviews Are Enough?: An Experiment with Data Saturation and Variability,” *Field methods*, vol. 18, no. 1, pp. 59–82, 2006.

[28] S. B. Thomson, “Sample Size and Grounded Theory,” vol. 5, no. 1, 2011.

[29] B. E. Neubauer, C. T. Witkop, and L. Varpio, “How phenomenology can help us learn from the experiences of others,” *Perspect. Med. Educ.*, vol. 8, no. 2, pp. 90–97, Apr. 2019.

[30] D. E. Polkinghorne, “Phenomenological Research Methods,” in *Existential-Phenomenological Perspectives in Psychology*, Springer US, 1989, pp. 41–60.

[31] J. W. Creswell and C. Poth, *Qualitative Inquiry and Research Design: Choosing Among Five Approaches (Google eBook)*. 2012.

[32] F. D. Davis, “Perceived usefulness, perceived ease of use, and user acceptance of information technology,” *MIS Q. Manag. Inf. Syst.*, vol. 13, no. 3, pp. 319–339, 1989.

[33] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, “User acceptance of information technology: Toward a unified view,” *MIS Q. Manag. Inf. Syst.*, vol. 27, no. 3, pp. 425–478, 2003.

[34] T. A. M. Spil, R. W. Schuring, and M. B. Michel-Verkerke, “USE IT: The theoretical framework tested on an electronic prescription system for general practitioners,” in *E-Health Systems Diffusion and Use: The Innovation, the User and the USE IT Model*, IGI Global, 2005, pp. 147–176.

[35] ENISA, “ICT security certification opportunities in the healthcare sector,” 2018.

[36] A. Papazafeiropoulou and K. Spanaki, “Understanding governance, risk and compliance information systems (GRC IS): The experts view,” *Inf. Syst. Front.*, vol. 18, no. 6, pp. 1251–1263, Jun. 2016.

[37] J. A. Wheeler, “Transform Governance, Risk and Compliance to Integrated Risk Management,” *Gartner*, no. May, 2016.

[38] J. B. S. dos Santos-Neto and A. P. C. S. Costa, “Enterprise maturity models: a systematic literature review,” *Enterprise Information Systems*, vol. 13, no. 5. Taylor and Francis Ltd., pp. 719–769, 28-May-2019.

[39] A. Blondiau, T. Mettler, and R. Winter, “Designing and implementing maturity models in hospitals: An experience report from 5 years of research,” *Health Informatics J.*, vol. 22, no. 3, pp. 758–767, Sep. 2016.

[40] C. Rosenstock, R. S. Johnston, and L. M. Anderson, “Maturity model implementation and use,” *ORganizational Project Management*, 2000. [Online]. Available: https://www.pmi.org/learning/library/maturity-model-implementation-case-study-8882. [Accessed: 11-Jun-2021].

[41] J. Becker, R. Knackstedt, and J. Pöppelbuß, “Developing Maturity Models for IT Management,” *Bus. Inf. Syst. Eng.*, vol. 1, no. 3, pp. 213–222, May 2009.

[42] C. V. Weber, B. Curtis, and M. B. Chrissis, “Capability Maturity Model, Version 1.1,” *IEEE Softw.*, vol. 10, no. 4, pp. 18–27, 1993.

[43] J. Poeppelbuss, B. Niehaves, A. Simons, and J. Becker, “Maturity Models in Information Systems Research: Literature Search and Analysis,” *Commun. Assoc. Inf. Syst.*, vol. 29, no. 1, pp. 505–532, Nov. 2011.

[44] A. Rabii, S. Assoul, K. Ouazzani Touhami, and O. Roudies, “Information and cyber security maturity models: a systematic literature review,” *Information and Computer Security*, vol. 28, no. 4. Emerald Group Holdings Ltd., pp. 627–644, 01-Oct-2020.

[45] T. Mettler, “Maturity assessment models: a design science research approach,” *Int. J. Soc. Syst. Sci.*, vol. 3, no. 1/2, p. 81, 2011.

[46] P. B. Seddon and R. Scheepers, “Towards the improved treatment of generalization of knowledge claims in IS research: Drawing general conclusions from samples,” *Eur. J. Inf. Syst.*, vol. 21, no. 1, pp. 6–21, 2012.

[47] E. M. Rogers, *Diffusion of Innovations. Free Press, New York. - References - Scientific Research Publishing*. 1983.

[48] D. R. Compeau and C. A. Higgins, “Computer self-efficacy: Development of a measure and initial test,” *MIS Q. Manag. Inf. Syst.*, vol. 19, no. 2, pp. 189–210, 1995.

[49] G. C. Moore and I. Benbasat, “Development of an instrument to measure the perceptions of adopting an information technology innovation,” *Inf. Syst. Res.*, vol. 2, no. 3, pp. 192–222, 1991.

[50] R. J. Hill, M. Fishbein, and I. Ajzen, “Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research.,” *Contemp. Sociol.*, vol. 6, no. 2, p. 244, Mar. 1977.

[51] R. L. Thompson, C. A. Higgins, and J. M. Howell, “Personal computing: Toward a conceptual model of utilization,” *MIS Q. Manag. Inf. Syst.*, vol. 15, no. 1, pp. 125–142, 1991.

[52] R. J. Hill, M. Fishbein, and I. Ajzen, “Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research.,” *Contemp. Sociol.*, vol. 6, no. 2, p. 244, Mar. 1977.

10 Appendix

10.1 Appendix A: Problem investigation interview questions

General information

1. Do you consent to me recording the audio of this interview? The purpose of the recording is so that I can transcribe the interview and the recordings will be deleted after the research is over.
2. Can you briefly introduce yourself? (Important is occupation, company and work experience)

Security certification

3. Why is it essential to incorporate information security certifications?
4. What challenges do you experience regarding security certification?
5. Could you describe the information security certification process?

Show and explain the diagrams that I created depicting the certification challenges.

6. How do these figures relate to your process and experiences regarding security certification? (Accurate depiction of the situation, why or why not?)
7. To what degree do sector-specific information security certifications overlap with each other?

Explain treatment candidates such as no certification, but hire additional compliance officers to accommodate continuous audits, acquire all certifications, component certification or construct your own control framework.

8. Which of the strategies from the field are most and least promising? Please explain why. Follow-up question about other candidate solutions that I might not have considered yet.
9. What (dis)advantages do you see for the different strategies?
10. What potential conflicts of interests could be relevant among the stakeholders?

10.2 Appendix B: Treatment Design Interview Questions

10.2.1 General interview questions

General information

1. Do you consent to me recording the audio of this interview? The purpose of the recording is so that I can transcribe the interview and the recordings will be deleted after the research is over.
2. Can you briefly introduce yourself? (Important is occupation, company and work experience)

Security certification

Explain Innovalor's perspective regarding continuous auditing demands and the financial burdens associated with information security certification

3. Do you recognize these issues or is the situation different in your eyes? (Ask for explanation)

Explain the four strategies and for each of them, ask the following three questions:

4. What are the advantages and disadvantages of this strategy?
5. In which situations would this be an effective strategy? (Which factors influence the selection?)
6. What potential conflicts of interests could be relevant among the stakeholders?

End with the following general question

7. Are there any strategies that I have not considered?

10.2.2 Stakeholder-specific interview questions

Auditor

1. How would the strategies affect the IT auditors? (Income, desirable or not?)
2. Is it possible that the security certification industry will develop towards an organization-wide baseline that are extended by specific in-depth components/modules?
3. Would a security certification that is scoped such that it only covers areas are not already covered by already acquired certification be possible in practice? Why or why not and when?
4. Is it always meaningful to work with accredited auditors? Why or why not?
5. Why does Innovalor have an ISO and eIDAS certification, when it might have been better to get just one SOC 2 assurance report instead? (Would SOC 2 be accepted across sectors?)
6. Is it indeed the case that an ISO 27001 audit does not consider whether controls are working effectively to the same extent as, for example, a SOC 2 audit? (If so, is a generic security baseline as a solution feasible?)

Standardization body

1. Why is there no single cross-sector information security standard?
2. Given the increase in outsourcing, are component certifications an effective solution or do you see the field developing in a different direction? (Feasibility of component certification)
3. How do you view the concept of assessing whether the internal control measures are designed properly, whether they are present and whether they are working effectively (opzet, bestaan en werking in Dutch)?

Technology provider

1. What does the security certification landscape look like in your organization?
2. What promising solutions do you see?
3. Which certifications are you certified for and why those?

10.3 Appendix D: Validation Briefing

We have constructed an information security certification maturity model to assist technology providers in choosing the appropriate certification strategy based on context. The model shows a high-level overview of certification maturity in general and provides guidelines for maximizing maturity within a given scenario.

In our view, a technology provider can operate in either many or few sectors and can have either few or many customers, resulting in four possible scenarios:

- **Few sectors, few customers:** The scenario for startups with limited resources that have not yet been able to generate many customers.
- **Few sectors, many customers:** The scenario for niche SMEs that have grown out of the startup phase by generating more customers, but are still restricted to operating in a small number of sectors.
- **Many sectors, few customers:** The scenario for SMEs that are expanding and branching out into new sectors, exposing themselves to sector-specific certification entry-barriers or significant audit overhead.
- **Many sectors, many customers:** The scenario for larger organizations that have expanded their services across sectors and accumulated a relatively large pool of customers, exposing themselves to higher levels of complexity regarding the management of certifications.

We define the following five certification strategies, which have been mapped onto their corresponding scenarios (based on our interpretation):

- **No certification by an independent third party**: Refrain from acquiring certification by an independent third party and accept additional audit overhead.
- **Sector-specific certification**: Adopt the most desirable sector-specific certification based on customer demands.
- **Common Denominator:** Certify a common denominator of sector-specific security controls, ideally auditing once to comply with many standards.
- **All certifications:** Minimize audit overhead by acquiring all relevant certifications (as per customer demand) to satisfy the customers' security demands, regardless of the sector-specific nature or overlap with existing certifications.
- **Component certification:** A general organization-wide security baseline supplemented by specific in-depth product and/or process certification(s).

Besides that, we define four general optimization practices, which are separate from the abovementioned strategies. These optimization practices can be utilized in conjunction with any of the previously mentioned strategies. They act as supplementary tools to yield more efficient certification processes:

- **Parallel audits:** Conduct several audits of different information security standards to avoid having to endure repetitive audits.
- **GRC tooling:** Utilize Governance, Risk & Compliance tooling to reduce the complexity and improve the efficiency of managing certifications.
- **Leverage certifications in negotiations:** Leverage the reduction in audit overhead due to the acquisition of appropriate certification to assume a favorable negotiation position.
- **Diversify certifications into sub-components:** Diversification of acquired certifications by splitting them up into several smaller sub-components with their own separate scopes.

In order to avoid confusion, we have put these nine concepts (five strategies + four optimization practices) in perspective by providing framework in which we place these in their appropriate context (Figure 1, located on page 2 of this document). The framework provides a graphical representation according to our understanding and functions as a steppingstone for getting to the certification maturity model.

Show the framework where the strategies are placed in context on the next page (page 2).

Now that the background has been properly explained, we would like to introduce the maturity model. We define the model as a high-level certification maturity metamodel, indicating the overall level of maturity of the certification concepts discussed in this thesis. It aims to assist technology providers in the decision-making process when considering an appropriate strategy for acquiring new certifications and managing existing ones. Higher maturity is not always better, as the desirable maturity level depends on the situation.

We define maturity as the degree to which certification processes are structured such that a technology provider can satisfy its customers' security demands. The model serves two purposes:

- It can indicate how technology providers can improve the maturity of their information security certification strategies to positively affect the value of the business and/or processes (development roadmap).
- It can help in the decision-making process when considering an appropriate strategy for acquiring new certifications and managing existing ones, based on the context in which a technology provider operates.

The **vertical axis** depicts six (including level 0) maturity levels that we adapted from the original capability maturity model. The **horizontal axis** depicts the different scenarios that a technology provider can operate in, as described on page 1 and illustrated on page 2 of this document.

The six **maturity levels** that were adapted from the original capability maturity model (CMM) are defined as follows:

0. Non-existent → No certification, but might involve informal structuring of processes.
1. Initial → First certification is acquired, but no standardized processes are in place.
2. Repeatable → Cross-sector compliance is achieved, but lacks depth.
3. Defined → Standardized certification procedures, but a high degree of complexity.
4. Managed → Reduced complexity through incorporating an individualized approach.
5. Optimized → Processes are structured such that overlap among certifications is mitigated and certifications provide meaningful contributions on top of each other.

Lastly, when answering the questionnaire questions, assume you are considering the most appropriate strategy for acquiring new information security certifications or managing existing ones in the context of a technology provider. Imagine that you would use the model to aid in the decision-making process.

The certification maturity model that we would like you to validate is located in Figure 2 on the last page of this document. The questionnaire ends with two open questions where you can leave your feedback. If you have any comments or remarks when answering the questionnaire, feel free to express these at the last two questions.

Show the certification maturity model on the next (last) page.

10.4 Appendix C: Treatment Validation Questionnaire (UTAUT)

10.4.1 Part one: Open questions

1. In your view, do you recognize the certification strategies and optimization practices outlined in the maturity model? If you do not recognize any, could you explain which ones you do not recognize?
2. In your view, are the strategies in the appropriate location in terms of level and order? If not, could you explain how you would locate them?

10.4.2 Part two: Validation questionnaire

Construct	Corresponding items	Source
Stakeholder type (multiple choice)	Which stakeholder type do you consider yourself to fit under the most? **S1.** Technology provider **S2.** IT auditor **S3.** Standardization agency **S4.** IT consultant **S5.** Other… (fill in yourself)	
Performance Expectancy (Measured with a 5-point Likert scale)	*Assume you are considering the most appropriate strategy for acquiring new information security certifications or managing existing ones in the context of a technology provider. Imagine that you would use the model to aid in the decision-making process.* **P1.** I would find the maturity model useful in my job. **P2.** Using the maturity model enables me to accomplish tasks more quickly. **P3.** Using the maturity model increases my productivity.	[32], [33], [34], [47], [48]
Effort Expectancy (Measured with a 5-point Likert scale)	**E1.** My interaction with the maturity model would be clear and understandable. **E2.** It would be easy for me to become skillful at using the maturity model. **E3.** I would find the maturity model easy to use.	[32], [33] [34], [49],
Attitude Towards Using Technology (Measured with a 5-point Likert scale)	**A1.** Using the maturity model is a good idea. **A2.** The maturity model makes work more interesting. **A3.** Working with the maturity model is fun. **A4.** I like working with the maturity model.	[33], [34], [48], [50], [51]
Social Influence (Measured with a 5-point Likert scale)	**S1.** People who influence my behavior think that I should use the maturity model. **S2.** People who are important to me think that I should use the maturity model.	[33], [34], [52], [51]
Facilitating Conditions (Measured with a 5-point Likert scale)	**F1.** I have the resources necessary to use the maturity model. **F2.** I have the knowledge necessary to use the maturity model. **F3.** The maturity model is not compatible with other systems I use.	[33], [34], [52], [51]

Self-Efficacy (Measured with a 5-point Likert scale)	*I could complete a job or task using the maturity model…* **S1.** If there was no one around to tell me what to do as I go. **S2.** If I could call someone for help if I got stuck. **S3.** If I had a lot of time to complete the job for which the maturity model was provided. **S4.** If I had just the built-in help facility for assistance.	[33], [34], [48]
Anxiety (Measured with a 5-point Likert scale)	**AN1.** I feel apprehensive about using the maturity model. **AN2.** The maturity model is somewhat intimidating to me.	[33], [34], [48]
Behavioral Intention to Use the System (Measured with a 5-point Likert scale)	**B1.** I intend to use the maturity model in the next 6 months.	[33], [34]
Feedback (Open question)	**F1.** In your view, are there any shortcomings of this model? **F2.** In your view, how could the maturity model be improved?	