UTRECHT UNIVERSITY

MASTER'S THESIS

Clearing the Cloudiness of SaaS: A SaaS Continuity Control Certification Framework

Author:
Nicholas XAVIER
6073409

Supervisors:
Dr. Slinger JANSEN
Dr. Sergio España CUBILLO

A thesis submitted in fulfillment of the requirements for the degree of Master of Science

in the

Business Informatics
Department of Information and Computing Sciences

August 4, 2020

"What kind of Mickey Mouse job is that? If you are going to do something then do it properly."

Martin Xavier

UTRECHT UNIVERSITY

Abstract

Clearing the Cloudiness of SaaS: A SaaS Continuity Control Certification Framework

by Nicholas XAVIER
6073409

Within the inter-dependent hierarchical structure of the cloud, its foundation, data centers, store data from Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) providers who offer their services as computing utilities. The SaaS business model offers SaaS customers with software solutions along with the required computing infrastructure, all within a quick and easy to install, and supposedly cheap package. Small and medium SaaS customers are typically not aware or do not have the resources to assess the risks involved when entering into a potential vendor lock-in situation with a SaaS provider. The unseen risks become evident when a SaaS provider's services stop as a result of a disruption event (natural or man-made), or bankruptcy. Only when a SaaS customer is unable to access their data and services are continuity options for their SaaS services queried. Loss of business-critical data and services can mark the beginning of the end for these businesses. As such, it is beneficial to all parties within the SaaS ecosystem to raise awareness of continuity risks by certifying SaaS providers through an assessment of the risk level associated with their system's continuity controls. Successfully doing so can improve SaaS customers' trust in the services they consume, and improve the overall health of the ecosystem. To achieve this, a research approach consisting of a multivocal literature review (MLR), expert evaluations, and case studies is applied to create and evaluate a SaaS continuity control framework. and two case studies to create and evaluate a SaaS continuity control framework. This framework assesses eight domains within a SaaS system using 125 questions to extract insights used to award a risk assurance certification mark. The promising evaluation of this framework demonstrates the ability of the applied scientific methodology, methods, techniques, and tools in the creation of a security control certification framework. The SaaS continuity control framework can be downloaded from www.saascontinuityframework.com, allowing practitioners to benefit from its useful insights.

Keywords: Cloud Security Controls, Software-as-a-Service, Risk Assessment, Business Continuity, Disaster Recovery, Certification Framework

Acknowledgements

Firstly, a big thank you to my primary supervisor, Dr. Slinger Jansen, for being a great resource for comparing my thoughts to those of an experienced and accomplished professional and academic. Also, the continuous laughter and humor we shared during this experience eased the burden of stress and anxiety, especially during the pandemic. The feedback from my second supervisor, Dr. Sergio España Cubillo, has been vital in adding finesse to the thesis with fresh ideas. As for my thesis buddy/ wife, Patzi Gieske, I could not have achieved this level of quality in my thesis without you! You weren't only a great work partner, but an awesome friend! You listened to me complain and motivated me when it seemed like I could not push through the seemingly endless pile of stress and new challenges. If our previous successes in the projects we worked on together were not enough, this experience boldly signifies that we make a great team!

Alexia Balatsoukas, my sweetheart! The degree of gratitude I have for the support and motivation you have endlessly provided for me during our time together can not be expressed in words! I simply could not have achieved what I have without you! Thank you for continuously knocking sense into me when I blew things out of portion and giving me the care I needed when life weighed heavily on me! You have my heart, love you! For my friends in Europe, thank you all for being such genuine and caring souls! You all have added your own individual spice to my melting pot of European experiences. For my family and friends in Trinidad and Tobago, thank you for being patient with me and lending your ears to hear my problems! Thank you, Mom and Dad for the continuous support and endless belief in my ability! Thank you for never letting me forget you are there for me! Love you both!

Contents

Chapter 1

Introduction

Cloud computing allows for information and communication technology (ICT) infrastructure and services to be spread across many organizations and locations across the globe. While minimizing the risk of single points of failure, it increases the challenge of protecting every cloud service (Arean, 2013). Bessemer Venture Partners et al. (2020, p. 9) predicts that, "[by] 2025, we expect the cloud to penetrate 50% of enterprise software. At the same growth rate, we predict that cloud will power 83% of software by 2030." The cloud is structured in a hierarchical manner, consisting of four layers stacked on top of one another. Starting with the foundation, data centers provide the hardware that the supports the cloud. It integrates the infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS) layers to provide these as services as utilities. However, the distinctions between these layers are not clearly defined, as components and features of one layer can be considered as part of another (Tsai, Sun, and Balasooriya, 2010). This presents a challenge as it becomes increasingly difficult to develop a clear picture of who and what is behind the cloud services used.

The SaaS business model's appeal arises from the reduced time to achieve a positive return on investment, increased connectivity, lower up-front costs, scalability, integration, and ease of adoption (Tang and Liu, 2015; Ma, 2007). Allowing SaaS providers to offer customers a software solution and the computing infrastructure required to run the solution. Creating a high degree of operational dependency of the SaaS customer on the SaaS provider's services. In many cases, this dependency has an unknown level of risk, specifically regarding the availability of data and services. Armburst et al. (2010) listed business continuity and availability of cloud services as the top obstacles for growth in the cloud industry. Business continuity involves the maintaining of continuous business operations before, during, and after disruptive events (Snedaker and Rima, 2013). ISO (2019, sec. 3.10) defines a disruption event as an "incident, whether anticipated or unanticipated, that causes an unplanned, negative deviation from the expected delivery of products and services according to an organization's objectives." Most SaaS providers do not offer guarantees of service continuity of their SaaS solutions by default (Van De Zande and Jansen, 2011). SaaS providers see these guarantees as a responsibility of the end-users, claiming that this is part of the practice of risk management which is an aspect of every business venture (De Jong, Jansen, and Overbeek, 2019). Consequently, a concept can be elicited from the need for the guaranteeing of the continuation of services, a continuity guarantee. As no clear definition of a continuity guarantee could be found, the study combines the definition of a business continuity plan, with knowledge gathered from literature to define it within the study's context. A **SaaS continuity guarantee** is a type of insurance offered by a SaaS provider to a SaaS customer, that stipulates the details about the availability of data and services in the event of a disruption in the SaaS supply chain (Cerullo and Cerullo, 2004; Van De Zande and Jansen, 2011; Snedaker and Rima, 2013).

SaaS providers generally lack benchmarks for measuring and communicating the benefits and risks of their services to potential customers. Disruption events can not always be foreseen by the providers and risk analysis is difficult for customers causing inaccuracies in determining return on investment, resulting in poor evidence supporting the investment in a SaaS continuity guarantee. The low level of transparency can be improved by increasing risk awareness and strengthening the trust between the SaaS providers and their customers (Sunyaev and Schneider, 2013). Increasing awareness can increase the demand for SaaS continuity guarantees, generating more revenue for the SaaS providers. SaaS customers need to assess SaaS continuity guarantees to identify the level of suitability to the organization's situation to make the best decision. Thus creating an opportunity to proactively assess SaaS continuity guarantees and supporting controls. This can be done through a third-party awarding certification marks to SaaS providers, which in turn eases the resources required by their customers to fulfill such an assessment (Sunyaev and Schneider, 2013; De Jong, Jansen, and Overbeek, 2019; Pauley, 2010; Van Velzen, De Jong, and Jansen, 2019). Investing in such mechanisms contributes to the ICT governance of the SaaS provider, positively impacting the share value of the organization (Stanton, 2005).

The low transparency of the SaaS industry supports the need for introducing a SaaS continuity controls certification mark. This certification mark has potential economic benefits for SaaS providers through an increase in the demand for SaaS continuity guarantees, while boosting SaaS customer risk awareness and trust, ultimately improving the overall health of the industry. Evidence of this projected impact can be seen in the E-commerce industry. An increase in trust induced by the introduction of certification marks reduced the demand for further legislation, and the hesitation of new users to adopt (Pauley, 2010).

1.1 Problem Statement

The complex interdependent nature of SaaS creates a low level of transparency, preventing customers from easily identifying which organizations support their SaaS solutions, their ability to maintain the availability of their services, and the full scope of risks involved (Anisetti et al., 2016). ORACLE and KPMG (2020) surveyed 145 organizations and reported the following consumption rates of SaaS for business-critical solutions: in 5% of organizations, SaaS consumes less than 10%; in 25% it consumes 10% - 20%; in 34% it consumes 21% - 30%; in 17% its consumes 31% - 40%; in 13% it consumes 41% - 50%; in 5% it consumes more than 50%; and the remaining 1% do not know their consumption rates. With (Bessemer Venture Partners et al., 2020)'s forecasts of cloud growth, it can be expected that the consumption of business-critical solutions will also grow. The availability of the a SaaS solution relies on the strength of the entities in the SaaS supply chain to recover from disruptions in their services (Van Velzen, De Jong, and Jansen, 2019).

Examples of a devastating disruption event in the cloud supply chain, can be seen the case of cloud service providers (CSP), *The Linkup*, and *2e2*. In August 2008, *The Linkup* reported losing access to approximately 45% of its customer's data and informed its 20,000 customer that their services will no longer be available (Armburst et al., 2010). This was due to *The Linkup's* reliance on another organization's (*Nirvanix*) data storage services. *Nirvanix* failed to transfer customer files to the system that hosted *The Linkup* causing the disruption (ITPro, 2008). In 2010, the borough of Waltham Forest in London, entered into a deal with cloud hosting provider, *2e2* for providing the full cloud infrastructure needed to support their ICT services. In 2013, the borough decided to go live with *Microsoft Dynamics* to support their interactions with the public for the 2013 London Olympics. Soon after the Olympics, despite conducting a financial investigation into the organization, the CIO of the borough received a sudden notice that *2e2* entered into administration due to financial difficulties (Preez, 2015). Paul Golland, the CIO of the borough, stated:

> I got a phone call telling me that the provider had gone under. And I can tell you, having to go and see members that basically can barely understand how their email system works that suddenly that the data centre provider had gone, all of our systems, some 160 servers, and this Dynamics environment that we had been developing, major interfaces, had all gone under, wasn't easy (Preez, 2015, prara. 5).

The borough was then notified that in 24 to 48 hours all services will be turned off (Preez, 2015). These cases show the devastation that can occur when cloud companies do not have strong continuity plans and their customers do not request continuity guarantees.

Organizations with mature ICT departments demand SaaS continuity guarantees by their SaaS providers (Alshammari, Alwan, and Alshaikhli, 2016). Whereas small and medium enterprises (SME) lacking this level of ICT maturity are typically unaware of the risks involved in the complex and interdependent structure of SaaS supply chains. A SaaS customer's difficulty in measuring risks associated with a SaaS solution prevents the customers from accurately determining the return on investment of SaaS continuity guarantees. Ultimately, decreasing their motivation to adopt a SaaS continuity guarantee, causing the SaaS provider to miss out on a potential revenue stream (Stanton, 2005). In many cases, the value of investing in a SaaS continuity guarantee is only realized when a disruption event occurs and the organization incurs damages. The general population has grown accustomed to high levels of availability from large enterprises such as Google. This high standard is now expected from all CSPs, regardless of maturity (Armburst et al., 2010). Resulting in amplified damages on user trust and brand reputation when sub-par handling of business disruptions are discovered. In the end, the SaaS customer and SaaS provider suffer.

1.1.1 Research Aim

By using the design problem template presented in Wieringa (2014), the below goal statement has been formulated to clarify the problem context, artefact, requirements, and desired impact of the study.

> **Goal Statement:** This study's aim is to *improve* the transparency of the SaaS industry *by* designing and evaluating a certification framework *that can* be used to analyze SaaS continuity control risks, and award certification marks to SaaS providers, *in order to* foster improvements in risk awareness and customer trust in SaaS.

1.1.2 Research Questions

In alignment with the goal statement, the main research questions (MRQ) and four sub-questions (SQ) are proposed in order to achieve the aim of the research. The evaluation criteria used in answering the questions are **bolded** and defined in Table 2.4.

MRQ: Can a framework be created that portrays the level of risk associated with SaaS continuity controls by analyzing a SaaS provider's ecosystem including the methods, tools, and processes used to support these controls?

SaaS customers may be unaware of the business continuity risks involved in using SaaS solutions and the continuity controls that support the solutions. Additionally, they may not have the resources required to conduct a thorough analysis of the controls. Diminishing their motivation to invest in SaaS continuity controls.

SQ1: What framework design features are best suited for scoring the risk associated with SaaS business continuity controls?

To ensure the **operational feasibility** and **ease of use** of the framework is appropriate, the correct layout, and operational procedure must be created. If the framework is too complicated and confusing, human errors may occur during its use.

SQ2: What business functions/ processes that support SaaS continuity controls should be analyzed in the certification framework?

There are a number **useful** methods, tools, and processes that support a SaaS provider's continuity controls that allow the adherence to agreements made in a SaaS continuity guarantee. If these supporting functions/ processes are not in place then a guarantee may contain empty promises.

SQ3: What SaaS continuity guarantee specific concepts should be analyzed in the certification framework?

In order to create an **effective** certification framework, a **complete** set of crucial SaaS continuity guarantee specific concepts must be identified and broken down into subconcepts. Providing further insights into the controls supporting the promise of guaranteed continuation of services for SaaS customers.

SQ4: What is a suitable scoring and evaluation method for the certification framework to correctly assess security controls?

Using the business functions and SaaS continuity control concepts, a scoring system should provide **useful** insights into the risk levels associated with different aspects related to SaaS continuity controls. It must also be flexible enough to adjust to changing technology and industry standards.

SQ5: What entities in the SaaS supply chain should be assessed?

The interdependence between supply chain entities involved in supporting SaaS operations means a business interruption at any entity can cause a domino effect impacting the operations of other supply chain entities.

SQ6: What are suitable criteria and requirements for evaluating the framework?

To improve the value of the final draft of the framework, a set of measures need to be identified from existing literature. These are used to determine how the framework compares to relevant artefacts and best practices, and provide appropriate means for experts to evaluate the framework. Ensuring that the decisions made in creating the framework add value.

1.2 Research Context

To provide clarity into the context of the research, a conceptual-model (Figure 1.1) has been created that visualizes the relevant concepts, attributes and relationships in this research's scope. A conceptual-model describes the general knowledge that is needed to understand the system and its context (Olivé, 2007). The application of the study's framework has been restricted to the Dutch ICT industry due to time and resource limitations. This has resulted in certain elements of the framework being designed to suit requirements that apply to the Netherlands. The knowledge needed to create this conceptual-model has been acquired during the preliminary research conducted during the problem investigation phase of this study. To assist in the readability of the conceptual-model, the concepts, attributes, and relationships are explained below.

Figure 1.1 describes a service ecosystem that is composed of customers and their service providers. In this ecosystem, service providers collaboratively create new services through continuous integration of various resources while exchanging services, ultimately adding value to the ecosystem (Guggenberger et al., 2020). A SAAS SOLUTION is a software product that contains the following characteristics: it is available through a web browser, does not require installation at the customer's location, does not require special integration and installation work, and is priced on the actual usage of the product (Mäkilä et al., 2010). In this study we look at three entities that support it, namely, CONTENT PROVIDERS, DATA CENTERS, and HOSTING PROVIDERS. The CONTENT PROVIDER is an external organization that provides products or services that are used by a SAAS SOLUTION (De Jong, Jansen, and Overbeek, 2019). DATA CENTERS are the locations where data are stored ,and the HOSTING PROVIDERS are companies that host technologies and services needed for the SAAS SOLUTION to be used over the Internet by SAAS CUSTOMERS.

The SAAS PROVIDER is the organization that provides a SAAS SOLUTION and SAAS CONTINUITY GUARANTEE to customers. Due to the interdependent nature of the cloud, the bankruptcy of a supply chain entity, natural disasters, Denial-of-Service attacks and other malicious attacks or simple programming bugs can cause an outage in a customer's SAAS SOLUTION as a whole or one of its functionalities (Dutta, Peng, and Choudhary, 2013). These disruptive create the need for SAAS SOLUTIONS to be supported by a type of insurance called a SAAS CONTINUITY GUARANTEE. The guarantee stipulates the details about the availability of data and services in the event of a business operation disruptions in the SaaS supply chain (Cerullo and Cerullo, 2004; Van De Zande and Jansen, 2011; Snedaker and Rima, 2013). It is typically implemented by the SAAS PROVIDER, and can include the involvement of third parties.

These guarantees include elements such as service level agreements (SLAs), source-code escrow, SaaS-escrow and SaaS guarantee funds (Van De Zande and Jansen, 2011). SLAs are legal documents the contain quality of service requirements, such as response time and throughput, that are agreed to by the SaaS provider and customer

(Patel, Ranabahu, and Sheth, 2009). However, SLAs do not contain agreements on disruption events that cause loss of access to data, the SAAS SOLUTION, and its support and maintenance. Source-code escrow or more specifically, SaaS-escrow, and SaaS guarantee funds contain contingency agreements in the event of loss of access. Source-code escrow is a contractual agreement where source code and other crucial documentation are held by a third-party called an escrow-agent (Freeman, 2004). This information is released to the client upon specific circumstances. The modified version of this, a SaaS-escrow, contains more features such as additional data-backups, and support and maintenance of the SAAS SOLUTION for a limited time (Van De Zande and Jansen, 2011). SaaS-escrows are not without their problems. For instance the SAAS CUSTOMER may not have the hardware or skills required to use the source-code, and if the SAAS SOLUTION has a large user base, then the escrow-agent may run into financial difficulty as the costs for hosting the solution may be too high (Van De Zande and Jansen, 2011). Another issue, is the generic and standardized nature of SaaS-escrows. For SAAS SOLUTIONS that use many third party CONTENT PROVIDERS, the SaaS-escrow may only offer coverage for the HOST PROVIDER, resulting in loss of potential business-critical features provided by the third parties (Van De Zande and Jansen, 2011). Due to high dependency of SAAS CUSTOMERS on SAAS PROVIDER, vendor lock-ins can occur,and with the pay-per-use model, SAAS PROVIDERS can typically forecast their financial outlook well into the future. This situation creates the opportunity for SaaS guarantee funds to be created. This fund is set up by the SAAS PROVIDER to cover the SAAS solution's costs to third parties to keep the services running for a period of time (Van De Zande and Jansen, 2011). This fund also acts as a separate legal entity free from the financial burdens of the SAAS PROVIDER.

To evaluate the risk level of this context, a CERTIFICATION FRAMEWORK is proposed. This framework is used to evaluate and score a SAAS PROVIDER based on an existing set of criteria with the intent to award the SAAS PROVIDER with a certification mark. The attributes of the CERTIFICATION FRAMEWORK concept have been derived from preliminary research and discussions with professionals known to the researcher. Financial outlook has been determined as a possible attribute through discussions held with professionals on the idea that one will not want to use a SaaS provider if the organization's financial outlook looks bleak. Legislation adherence has been determined necessary due to the implementation of GDPR and reading of Sunyaev and Schneider (2013). Disaster recovery plan and continuity plan testing are derived from the risk ontology presented in Dutta, Peng, and Choudhary (2013). The need for evaluating SaaS technology maturity came from conversations with the professionals on system bugs, and the availability of certified personnel in specific technologies. Data security measures has been a topic of discussion in a large number of cloud computing literature, which made it evident that it should be included in the framework. The completeness of the SAAS PROVIDER'S continuity guarantee arose from papers published by members of the Software Ecosystems research group, specifically Van De Zande and Jansen (2011) and Van Velzen, De Jong, and Jansen (2019). These attributes formed the initial vision of the framework which evolves during the progression of the study.

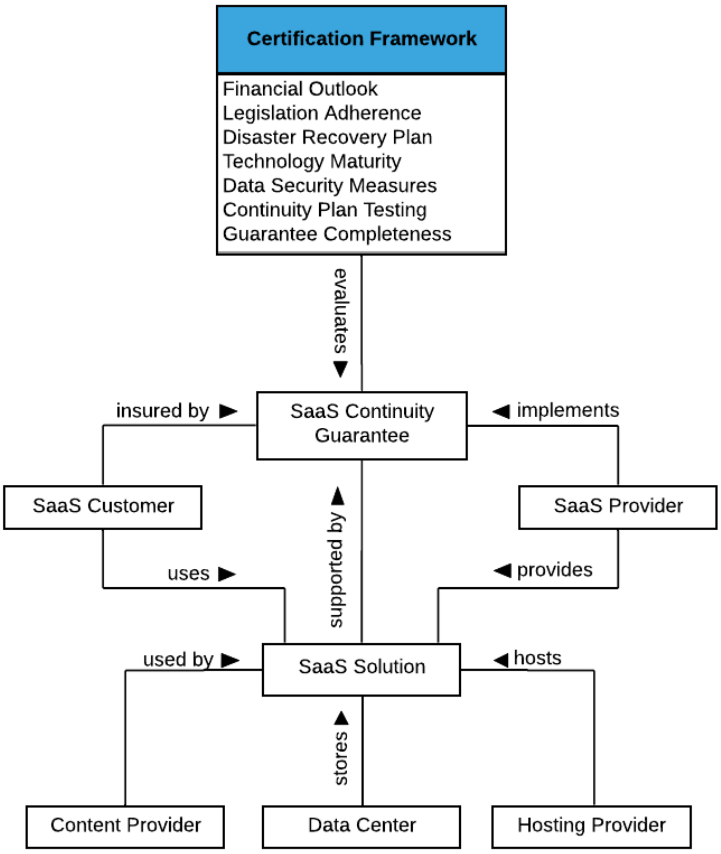


FIGURE 1.1: Research context conceptual-model version 1

1.3 Thesis Outline

Below contains brief descriptions of the information provided in the chapters of this study:
Chapter 2: Provides a details description of the research approach used and the methods and techniques implemented to achieve the aim of the study.
Chapter 3: Identifies the main concepts of the cloud ecosystem, and the security framework ecosystem applicable to the study's context.
Chapter 4: Discusses the relevant concepts and sub-concepts needed to create controls and questions for the materialization of the SaaS continuity control framework.
Chapter 5: Compiles the concepts identified in Chapters 3 and 4, with framework features to create the first draft of the SaaS continuity control framework.
Chapter 6: Examines the findings from the expert evaluations.
Chapter 7: Describes the changes made to the framework from the insights gained through the expert evaluations.
Chapter 8: Examines the results and insights from the case studies.
Chapter 9: Discusses the study's alignment with the research approach and threats to its validity.
Chapter 10: Summarizes the concluding reflection on the study's research questions and opportunities for future research.

Chapter 2

Research Approach

2.1 Introduction

This chapter describes in detail the research approach used in this study. It begins by discussing the choice of following the design science research (DSR) methodology and elaborates on how elements of this study fit into the methodology's life cycle. Three main research methods are then described: (1) a mulitvocal literature review (MLR) to identify possible characteristics and requirements of the framework design; (2) expert evaluations in the form of interviews as the first round of evaluations of the draft framework; and (3) multiple holistic case studies to evaluate the latest version of the framework. The compilation of the multiple process fragments to accommodate the needs of the study makes use of the teachings from the method engineering discipline. Guiding the study's attempts at designing, constructing, and adapting existing methods, techniques, and tools to create the desired certification framework (Brinkkemper, 1996). Method engineering employs the use of process deliverable diagrams (PDD) which are used to visualize the study's research approach, the framework's operational procedure, and the LinkedIN strategy used to source experts, all of which are found in Appendix A. A PDD consists of two integrated diagrams. The left side of the PDD shows the research process based on a unified modelling language (UML) activity diagram, while the right side of the PDD shows the deliverables based on a UML class diagram (Weerd and Brinkkemper, 2008).

2.2 Design Science Research

This study aims to design and evaluate a software as a service (SaaS) continuity control certification framework. This framework is envisioned to be a tool for assessing the risk level of SaaS continuity controls and awarding an appropriate certification mark based on the assessment results. To do this, the DSR methodology is adopted from Hevner and Chatterjee, 2010, and visualized in Figure 2.1. This grounds the study's attempt to produce a high quality and scientifically sound framework, in a proven methodology.

This methodology is appropriate as the framework being designed is aimed at improving real-world problems (Wieringa, 2014; Hevner and Chatterjee, 2010). Within the DSR, three sub-cycles are present, the *relevance cycle*, *design cycle*, and *rigor cycle*. These occur in iterations to build upon knowledge gained during each cycle. DSR begins with the *relevance cycle*, which provides the context, requirements, and acceptance criteria used in the evaluation of the research results. It also includes the field testing of the designs created in the *design cycle*. The *rigor cycle* creates the foundation for the DSR cycle through the review of literature and the generation of the knowledge base. The *design cycle* begins with the creation of framework design alternatives from the knowledge and experience gained through the *rigor cycle*. Flowing into the evaluation of the designs against the requirements and acceptance criteria from the *relevance cycle* until an acceptable design achieved.

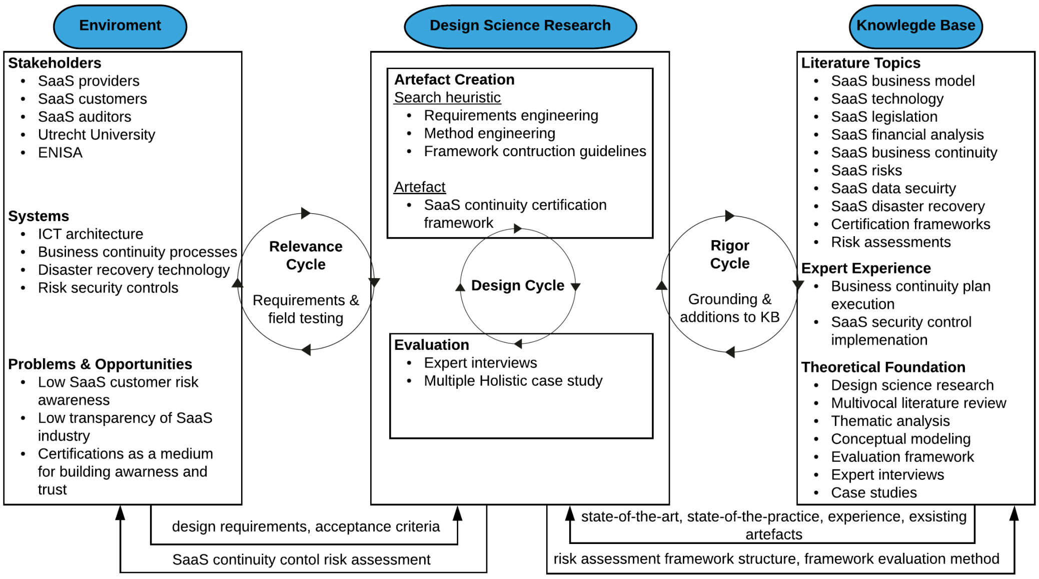

Enviroment
Design Science Research
Knowlegde Base
Stakeholders
• SaaS providers
• SaaS customers
• SaaS auditors
• Utrecht University
• ENISA
Systems
• ICT architecture
• Business continuity processes
• Disaster recovery technology
• Risk security controls
Problems & Opportunities
• Low SaaS customer risk awareness
• Low transparency of SaaS industry
• Certifications as a medium for building awarness and trust
Relevance Cycle
Requirements & field testing
Artefact Creation
Search heuristic
• Requirements engineering
• Method engineering
• Framework contruction guidelines
Artefact
• SaaS continuity certification framework
Design Cycle
Evaluation
• Expert interviews
• Multiple Holistic case study
Rigor Cycle
Grounding & additions to KB
Literature Topics
• SaaS business model
• SaaS technology
• SaaS legislation
• SaaS financial analysis
• SaaS business continuity
• SaaS risks
• SaaS data secuirty
• SaaS disaster recovery
• Certification frameworks
• Risk assessments
Expert Experience
• Business continuity plan execution
• SaaS security control implemenation
Theoretical Foundation
• Design science research
• Multivocal literature review
• Thematic analysis
• Conceptual modeling
• Evaluation framework
• Expert interviews
• Case studies
design requirements, acceptance criteria
SaaS continuity contol risk assessment
state-of-the-art, state-of-the-practice, experience, exsisting artefacts
risk assessment framework structure, framework evaluation method

FIGURE 2.1: DSR cycle applied to this research, adapted from Hevner and Chatterjee (2010, p. 16)

2.2.1 Research Methods

Within the iterative process of designing and evaluating the framework, the answers to the MRQ and its SQs mentioned in section 1.1.2 are revealed. The methods to generate these answers are displayed in Table 2.1. The first method used is an MLR to identify and map key concepts, and sub-concepts required to create an effective framework. The draft framework created is evaluated through expert interviews to gather feedback on its **operational feasibility**, **completeness**, **ease of use**, and **usefulness**. The MLR process is revisited to validate the feedback and explore newly discovered ideas in order to develop the next draft of the framework. Once a satisfactory framework is achieved, multiple case studies are conducted to determine the **effectiveness** of the framework is in a real-life situation (Shrestha, Cater-steel, and Toleman, 2014).

TABLE 2.1: Research methods used to answer the SQs

Method	SQ1	SQ2	SQ3	SQ4	SQ5	SQ6
Multivocal Literature Review	✓	✓	✓		✓	✓
Expert Evaluations	✓	✓	✓	✓	✓	
Multiple Holistic Case Studies	✓			✓		

2.3 Multivocal Literature Review Protocol

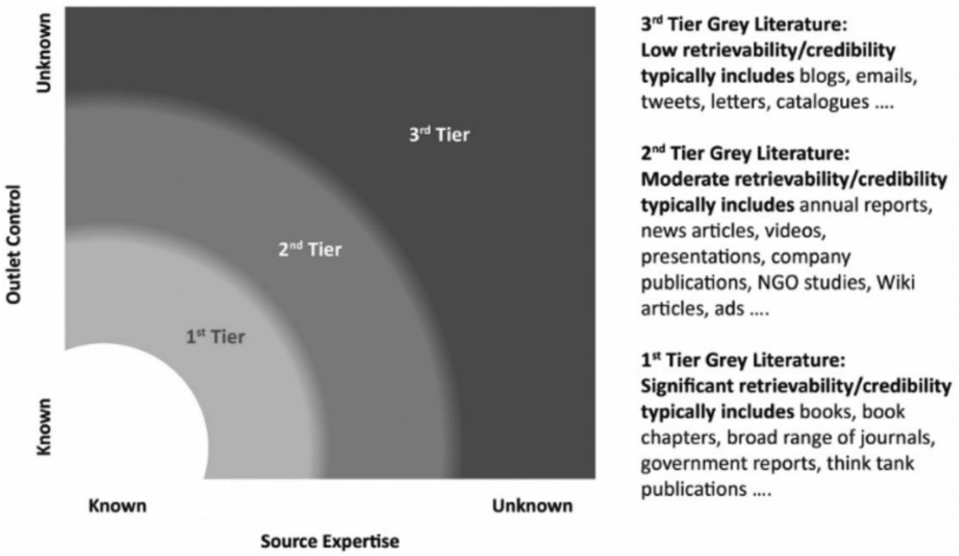
A literature review facilitates knowledge development, uncovers new research areas, and identifies the research areas needed for the creation of the SaaS continuity certification framework (Wohlin, 2014). Preliminary research into the problem domain began by reading accumulated literature by the Software Ecosystems Lab. Following the reading of the papers by Van Velzen, De Jong, and Jansen (2019) and De Jong, Jansen, and Overbeek (2019), who are also part of the Software Ecosystems Lab, it became clear that a limited amount of academic literature can be found regarding SaaS continuity guarantees. As a result, an academic and grey literature (GL) review is necessary to fill any gaps in knowledge left by the lack of academic literature. Incorporating GL allows a researcher to take advantage of a variety of positive contributions from material generated through the course of real-life practices (Adams, Smart, and Huff, 2017). Adams, Smart, and Huff (2017, p. 435) state, "[that] GL can bring the disparate voices of experience into scholarly conversation to increase its relevance and impact." This statement applies directly to the goal statement of this study seen in section 1.1.1. To incorporate academic and GL into the literature review, the guidelines for conducting an MLR presented in Garousi, Felderer, and Mäntylä (2019) are followed. Garousi, Felderer, and Mäntylä (2019) describes MLRs as a form of a systematic literature review that includes GL and published literature. The use of such guidelines improves the design of the framework by ensuring only credible literature is used and reducing the effects of research bias (Kitchenham, 2004).

2.3.1 Search Process and Source Selection

During preliminary research, a set of key concepts, attributes, and their relationships are identified and used to create the conceptual-model presented in Figure 1.1. These elements are the terms used with search engines such as Google, Google Scholar, ACM Portal and other search engines accessible through the Utrecht University library system. Search strings are improved by using Boolean statements such as AND and OR. Garousi, Felderer, and Mäntylä (2019) provides three possible stopping criteria for GL searches: (1) theoretical saturation; when no new concepts emerge from the search results, (2) effort bounded; only include the top N search engine hits, and (3) evidence exhaustion; all evidence has been extracted. For results from Google search queries, only the links from the first two pages are investigated. This forces quick refinements of search parameters, producing the most relevant grey literature sources. For applicable literature, snowballing is adopted in the development of the literature pool. Literature available from the Software Ecosystems Lab library has been used as the starting set for which backward and forward snowballing are applied. Wohlin (2014) describes backward and forward snowballing as:

> *Backward Snowballing:* Analyzing the reference lists of the starting set papers to identify new candidate papers for further reading.
>
> *Forward Snowballing:* Identifying new paper by analyzing the papers that cite the already examined and approved papers that are relevant to the research.

To determine the usefulness and relevance of academic literature, the researcher first read the abstract, then the introduction, and lastly, the conclusion before adding it to the literature pool. However, GL does not typically contain these academic elements and requires a more thorough review. GL is composed of knowledge and artefacts that have not passed through the rigor of scientifically sound publishing processes associated with published academic work (Lawrence et al., 2014). As GL is a broad term and contains a large variety of material, Figure 2.2 provides a visualization of the scope of GL acceptable for this study. In this study, literature from the 3rd tier is avoided due to low credibility. The credibility of the GL from the remaining tiers are assessed using the questions in Table 2.2.



3rd Tier Grey Literature:
Low retrievability/credibility
typically includes blogs, emails, tweets, letters, catalogues ....

2nd Tier Grey Literature:
Moderate retrievability/credibility
typically includes annual reports, news articles, videos, presentations, company publications, NGO studies, Wiki articles, ads ....

1st Tier Grey Literature:
Significant retrievability/credibility
typically includes books, book chapters, broad range of journals, government reports, think tank publications ....

FIGURE 2.2: Grey literature tiers, extracted from Adams, Smart, and Huff (2017, p. 435)

2.3.2 Quality Assessment

To ensure the relevance and credibility of the literature, a quality assessment checklist is used, including exclusion criteria. As suggested by Adams, Smart, and Huff (2017), the assessment is tailored to this research study as well as assessed by the researcher's supervisor and academic colleagues. Table 2.2 displays the evaluation criteria and the questions used to score the criteria. Literature that is either: (1) not related to the elements presented in Figure 1.1; (2) not written in English; or (3) not freely accessible, is excluded without scoring. Criteria questions are answered with a score of 1 for *Yes* and 0 for *No*, besides the *Outlet type*. *Outlet type* refers to the GL tiers in Figure 2.2 and are scored as seen in Table 2.2 (Adams, Smart, and Huff, 2017).

TABLE 2.2: Quality assessment checklist, adapted from Garousi, Felderer, and Mäntylä (2019)

Criteria	Questions
Related to concepts in Figure 1.1	• Is it related to one of the concepts?
Written in English	• Is the literature written in English?
Freely accessible	• Can the literature be read at no financial cost to the researcher?
Authority of the producer	

Continued on next page

Table 2.2 - continued

Criteria	Questions
	• Is the publishing organization reputable? • Is an individual author associated with a reputable organization? • Has the author published other work in the field? • Does the author have expertise in the area?
Methodology	• Does the source have a clearly stated aim? • Does the source have a stated methodology? • Is the source supported by authoritative, contemporary references? • Are any limits clearly stated? • Does the work cover a specific question? • Does the work refer to a particular population or case?
Objectivity	• Does the work seem to be balanced in presentation? • Is the statement in the source as objective as possible? Or, is the statement a subjective opinion? • Are the conclusions supported by the data?
Date	• Does the item have a clearly stated date?
Linkage of related sources	• Have key related grey literature or formal sources been linked or discussed?
Novelty	• Does it enrich or add something unique to the research? • Does it strengthen or refute a current position?
Outlet Type	• 1st tier GL (measure = 1): High outlet control/ High credibility: Books, magazines, theses, government reports, white papers. • 2nd tier GL (measure = 0.5): Moderate outlet control/ Moderate credibility: Annual reports, news articles, presentations, videos, Q/A sites (such as StackOverflow), Wiki article. • 3rd tier GL are not be used.

The scores from the quality assessment questions are summed and normalized by dividing the values by the number of questions. A threshold score of half the total number of questions is maintained. Once a literature's score is above the threshold, it is included in the literature pool. This review occurred in iterations as the knowledge base grew, requiring the rolling back of the Snowballing process to remove incorrectly added papers and adjust search parameters.

2.3.3 Data Collection

To correctly record the information gathered from the literature pool, a data collection form has been created using *MS Excel*. Inspiration for the form's design came from the publicly available MLR form presented in Garousi, Felderer, and Mäntylä (2019). A snippet of the data collection form used can be found in Appendix D.1. As the quality of the certification framework depends on the effectiveness of the data extraction in recording data (Garousi and Felderer, 2017). The form collects all the information required to answer the quality criteria questions in Table 2.2, and maps the extracted information to the relevant research questions and codes used in this study (Kitchenham, 2004). Since GL needs to be thoroughly read, *MS OneNote* is used to extract and codify quotes from the literature if deemed potentially useful.

2.3.4 Data Synthesis

This represents the beginning of requirement engineering activities aimed at identifying goals for, functions of, and constraints for the system under consideration

(Zave, 1997). To ensure that data synthesis generates the requirements, and relevant relationships for the certification framework, guidelines for conducting a thematic synthesis are followed from Cruzes and Dybå (2011). Braun and Clarke (2012) describes thematic synthesis as a method for systematically identifying, analyzing, and generating insights into patterns of meaning (themes) across a data set. For the certification framework, themes are seen as high-level concepts relating to SaaS continuity controls. During this process, sub-concepts are identified for the different high-level concepts. This method is suitable as it provides flexible procedures ideal for researchers new to systematic research, addresses research questions about need, appropriateness and effectiveness, and copes well with identifying patterns across the diverse topics presented in Figure 1.1 (Cruzes and Dybå, 2010; Cruzes and Dybå, 2011; Braun and Clarke, 2012). This thematic analysis follows guidelines by Cruzes and Dybå (2011) allowing the researcher to progressively interpret the data until a framework draft is possible. The different levels of this progression have been visualized in Figure 2.3.

In order to code the data, an integrated approach is taken. In this study, the concepts discovered through preliminary research (Figure 1.1) are used to initially code and interpret the data. As the research evolves, codes are added or modified, eventually transforming into high-level concepts. Low-level relationships are identified and mapped. Allowing a draft of the certification framework to materialize.

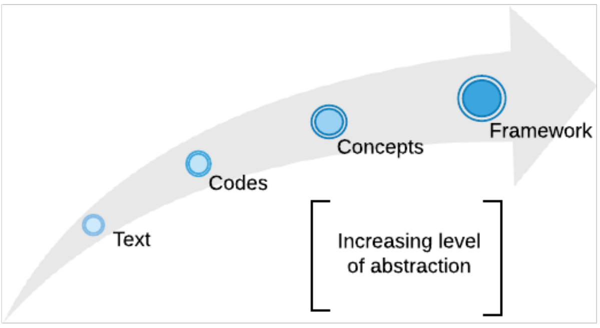


FIGURE 2.3: Levels of interpretation, adapted from

2.3.5 Framework Construction

With concepts and their relationships identified, the final step is the actual construction of the framework. To ground the framework's construction in scientific literature, guidelines for constructing a maturity model are adopted. Bruin et al. (2005, p. 1) describes these models as being "used as an evaluative and comparative basis for improvement and in order to derive an informed approach for increasing the capability of a specific area within an organization." Notably, the framework is not aimed at being a maturity model, however, there are similar characteristics between the envisioned framework and maturity models. As such, the guidelines adopted ensure that the desired characteristics are developed using best practices. The first four phases for constructing a maturity model as described in Bruin et al. (2005) are adopted and seen in Figure 2.4. The last two phases of *deploy* and *maintain* are outside the scope of this study and not displayed in Figure 2.4. The information that is intended to be discovered during these phases is compensated for by the sub-cycles seen in Figure 2.1.

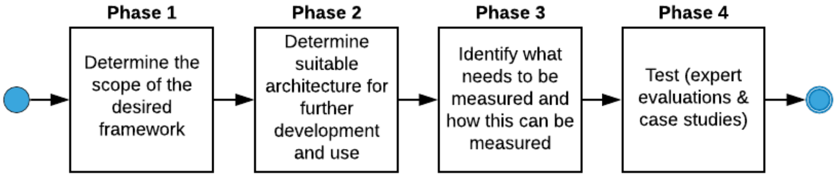

Phase 1
Determine the scope of the desired framework
Phase 2
Determine suitable architecture for further development and use
Phase 3
Identify what needs to be measured and how this can be measured
Phase 4
Test (expert evaluations & case studies)

FIGURE 2.4: Framework construction phases, adapted from Bruin et al. (2005)

Phase 1 The scope of the framework is defined in the *Literature Topics*, *Stakeholders*, and *Systems* lists in Figure 2.1. However, the depth of coverage into the literature topics is not defined. This is determined by the size of the literature content available and the strength of influence of each topic on achieving the aim of the study. The required granularity of information presented in the framework is identified and refined through expert evaluations.

Phase 2 By looking at existing frameworks, architectural features are identified and replicated. Based on the findings from the MLR, these features are modified to suit the questions that are posed to a SaaS provider in the framework.

Phase 3 What needs to be measured is identified through the thematic analysis and expressed as questions in the framework. The questions are answered using multi-leveled satisfaction answers seen in maturity models. Providing flexibility to account for a differing level of interpretation of the evidence presented by a SaaS provider in response to the questions.

Phase 4 In this study, this phase can be seen as the framework evaluation phase. It is explained in detail throughout Section 2.4.

2.4 Framework Evaluation

As mentioned in Section 2.2, DSR involves the creation and evaluation of an artefact. Evaluating a framework can be a challenging task as the design of the framework and process must be evaluated (Shrestha, Cater-steel, and Toleman, 2014). In order to correctly report this evaluation, the reporting model proposed by Shrestha, Cater-steel, and Toleman (2014) is adopted. This model presents the structure of the evaluation protocol in terms of: (1) its inputs which are the framework and the evaluation strategy used; (2) its outputs which cover the participants and the activities of the evaluation process; and (3) its outcomes from the evaluation in terms of immediate findings, their discussion, and long-term impacts. This reporting model has been adjusted to suit this study and is illustrated in Figure 2.5.

The feedback and insights gained from the evaluations are applied to the draft framework so that incremental improvements are made to the framework to form new versions (Hevner and Chatterjee, 2010). As the completion of the interviews depends more on the willingness and availability of the interviewees than the interviewer, the projected number of interviews and availability of interviewees changes

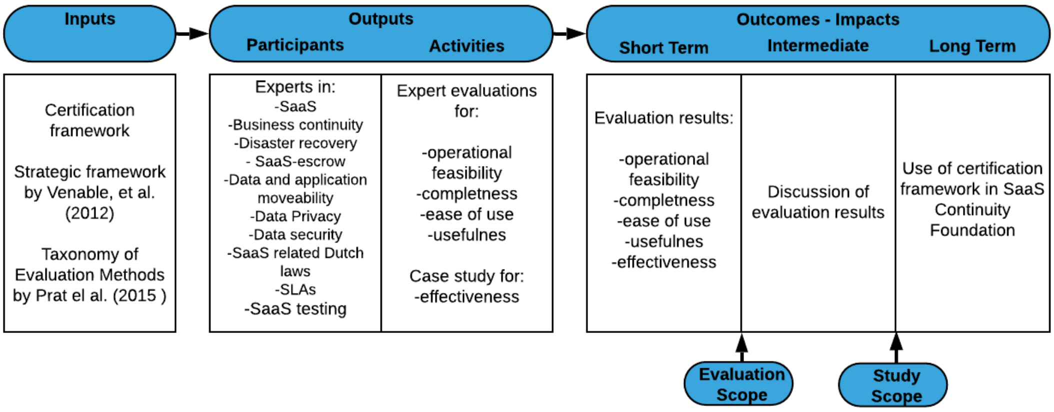


FIGURE 2.5: Reporting model, adapted from Shrestha, Cater-steel, and Toleman (2014, p. 280)

as the study progresses. For this reason, the increments consist of a varied number of evaluations. The decision for completing an increment is based on the feedback gathered, and the available time until the next milestone of the project plan.

Evaluation Strategy

Based on the artefact of this study, the methods of expert evaluations and multiple holistic case studies for artefact evaluation are used. However, to explore the suitability of these methods and others, the strategic evaluation framework by Venable, Pries-heje, and Baskerville (2012) is consulted. In Table 2.3, expert evaluation and case study methods are justified by this in the framework as *ex-ante* (prior to framework construction) and *ex-post* (after framework construction) respectively (Pries-Heje, Baskerville, and Venable, 2008; Venable, Pries-heje, and Baskerville, 2012).

TABLE 2.3: Evaluation strategy protocol, based on the research presented in Venable, Pries-heje, and Baskerville (2012)

Evaluation	**Evaluation setting**	**Evaluation method**	**Evaluation focus**	**Evaluation instruments**
Design product (Artefact)	Ex-ante, Artificial	Expert evaluation	Operational feasibility, completeness, ease of use, and usefulness of framework	Taxonomy of Evaluation Methods from Prat, Comyn-Wattiau, and Akoka (2015)
Design product (Artefact)	Ex-post, Natural	Case study	Effectiveness of framework in real life assessment	Taxonomy of Evaluation Methods from Prat, Comyn-Wattiau, and Akoka (2015)
Design process (Research method)	Ex-post, Artificial	Alignment with design science and MLR guidelines	Design Science methodology and MLR method	Guidelines for DSR evaluation from Shrestha, Cater-steel, and Toleman (2014) and acceptance criteria for conducting a MLR by Garousi, Felderer, and Mäntylä (2019)

In order to perform this evaluation, a set of criteria have been formulated. To support this selection, the guidelines and taxonomy presented in Prat, Comyn-Wattiau, and Akoka (2015) for selecting suitable criteria are used. The selected criteria provide the ability to evaluate the aim, structure, and use of the framework. The criteria definitions have been adapted to suit the context of this study and can be seen in Table 2.4.

TABLE 2.4: Evaluation criteria and definitions

Criteria	Definition by Prat, Comyn-Wattiau, and Akoka (2015)	Adapted definition for this study	Evaluation Tool
Usefulness	The degree to which the artefact positively impacts the task performance of individuals.	To what degree does the framework extract insightful information for awarding a certification mark?	5-point Likert scale
Ease of use	The degree to which the use of the artefact by individuals is free of effort.	What is the degree of difficulty associated with gathering the information required by framework?	5-point Likert scale
Operational feasibility	Evaluates the degree to which management, employees, and other stakeholders, will support the proposed artefact, operate it, and integrate it into their daily practice.	To what degree do the experts see the framework being used by individuals in practice?	Open-ended questions
Completeness	The degree to which the structure of the artefact contains all necessary elements and relationships between elements.	To what degree does the framework assess critical risk concepts relating to SaaS continuity controls, and contain necessary questions for adequately assessing these concepts?	Open-ended questions
Effectiveness	The degree to which the artefact achieves its goal in a real situation.	To what degree do insights gathered portray the level of risk associated with a SaaS continuity controls?	Open-ended questions

2.4.1 Expert Evaluations

In order to evaluate and improve the certification framework draft, semi-structured expert interviews are held. Interviews are useful for eliciting valuable feedback through the experiences and knowledge of experts during the early stages of framework development (Wieringa, 2014). The interviews are directed at gathering feedback aligned with the research questions and the evaluation criteria mentioned in Table 2.4. However, the effectiveness of the elicitation process during the interviews depends greatly on the quality of interaction between the participants (Zowghi and Coulin, 2005). To elicit information, open-ended questions and framework question evaluations using 5-point Likert scales are used. The 5-point scale is used to quantified the expert's opinions on the risk control questions in the framework. By doing so, questions can be identified as satisfactory, in need of modification, or should be removed. Additionally, during the framework question evaluation phase, protocol analysis is encouraged so that participants evaluate the questions whilst describing their thought process (Goguen and Linde, 1993). This creates an opportunity for brainstorming with the interviewees, which is an informal discussion aimed at rapidly generating ideas (Osborn, 1953). However, this combination of techniques and tools creates difficulty in completing the interview within the agreed upon time.

To ensure the effectiveness of the interviews, an interview protocol has been created and piloted prior to the interviews. This is used as an inquiry tool to elicit beneficial evaluations from experts about the draft framework (Patton, 2015). To ensure the interview protocol is anchored in the aims of the study, and that feedback gathered from the interviews are useful and relevant, it is important to form a systematic approach to creating the interview protocol. The main phases of the interview protocol refinement framework created by Castillo-Montoya (2016) have been followed and are seen in Figure 2.6. A snippet of the*MS Excel* sheet used to record the evaluation score of **ease of use** and **usefulness** can be found in Appendix

B.5.

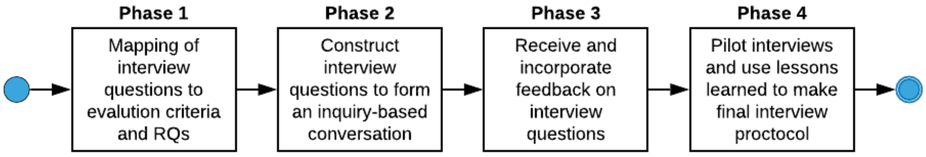

Phase 1
Mapping of interview questions to evalution criteria and RQs
Phase 2
Construct interview questions to form an inquiry-based conversation
Phase 3
Receive and incorporate feedback on interview questions
Phase 4
Pilot interviews and use lessons learned to make final interview proctocol

FIGURE 2.6: Interview protocol refinement framework phases, adapted from Castillo-Montoya (2016)

Phase 1 includes the mapping of interview questions to one or more of the evaluation criteria and SQs. This is done to increase the utility of the interview questions and ensure their relevance to the aim of study and its research questions. The mapping of questions to criteria and SQs, reveal gaps in what is being asked as well as unnecessary questions. Allowing the interviews to be conducted in an efficient and effective manner, minimizing the time required by the interviewee to participate. This phase also brought attention to the ordering of the questions. It is important that the interview flows in a natural way, starting with rapport building, leading into the key questions, hopefully eliciting the true perspectives of the interviewee (Patton, 2015). The matrix used for the mapping of interview questions to SQs and evaluation criteria can be found in Appendix B.4.

Phase 2 focuses on naturalizing the flow of the conversation around the interviewee's life experiences while asking specific questions about the research topic (Patton, 2015; Castillo-Montoya, 2016). This inquiry-based conversation contains the following characteristics: (1) the interview questions are different from the research questions; (2) the ordering of the questions follow the social rules of a normal conversation; (3) the questions vary in goal and topic; and (4) follow-up questions are included as well as impromptu questions.

Phase 3 requires the peer-reviewing of the interview protocol draft. By receiving feedback, modifications are made to enhance the overall quality of the interview protocol. The feedback is focused on the topics of: (1) the structure of the interview protocol; (2) the writing style; (3) the overall length of the protocol; and (4) the ease of understanding the questions. The feedback is gathered through colleagues in the Software Ecosystems Lab, and fellow master's in Business Informatics students. These groups are known to have experience in writing scientific interview protocols and have the ability to provide constructive feedback.

Phase 4 concludes the development of the final draft of the interview protocol by running a pilot interview. This pilot is conducted with an interviewee that has similar characteristics as the targeted interviewees. In this interview simulation, notes on the interviewer's experience are taken to improve the draft protocol and generate a final version.

Prior to each interview, the interviewee is provided with a research information sheet and interview consent form. These documents are based on templates created by TUDelft (2019). Before the start of an interview, conversations are held about aim of the study using the research information sheet, the structure of the interview, and the confidentiality of the information gathered from interview. The resulting interview protocol documents are found in Appendix B.

Expert Selection Criteria

To produce an effective framework, the expert selection needs to contain only relevant and experienced individuals. Thus requiring the use of purposive sampling. Purposive sampling deliberately chooses participants based on the qualities the participant possesses and useful when investigating new areas of research, and determine if further study is worth the effort (Etikan, 2016). This sampling method also emphasizes on the researcher finding people who are willing to provide the information by virtue of knowledge or experience. Etikan (2016) notes that this method can be expected to take a long time to produce conclusions.

The participants need to be professionally relevant, experienced, and able to communicate with the researcher. Resulting in the following expert requirements: (1) a prospective expert must have two years of experience in at least one of the framework's risk domain seen in Figure 3.5; (2) a prospective expert must speak English; and (3) able to conduct the interview online due to the COVID-19 pandemic. Prospective experts are identified through querying *LinkedIN* with keywords related to the concepts of the framework, and probing the *LinkedIN* network of the researcher's supervisor. Prospects unknown to the researcher or project supervisor are verified by scrutinizing their *LinkedIN* accounts and, if available, publications in the field. Additionally, authors (individuals and companies) of the GL used in the study are contacted using *LinkedIN* or E-mail.

LinkedIN Strategy

If used correctly, *LinkedIN's* professional network can be an effective research tool when acquiring research participants (Unkelos-Shpigel, Sherman, and Hadar, 2015). Allowing professional relationships to form quickly over the nearly instantaneous connections formed by the click of a button (Quinton and Wilson, 2016). To run an effective to promote the research and connect with potential interviewees, guidance has been acquire through GL sources. Balkhi (2018) provided four areas of focus: (1) make your profile stand out; (2) connect with people and interact; (3) join *LinkedIn* groups; and (4) post engaging content. With these areas in mind, a PDD of the LinkedIN campaign's activities used in the study has been created and can be found in Appendix A.3.

Interview Constraints

Due to the size of the framework draft, the estimated time for evaluating the entire framework has been placed above two hours. This can be seen as a potential repellant for interviewees. It is necessary to limit the completion time of the interview to one that the interviewee is willing to contribute. To do so, a form containing the risk domains and their estimated completion times is sent to each interviewee. The interviewees are instructed to select which risk domains they want to evaluate. From this, the form provides a total estimated interview completion time based on their selection. Once the interviewee agrees to the selection and resulting interview time, the necessary adjustments are made to the relevant interview documents to suit each interviewee's constraints. This domain selection and time estimation form is found in Appendix B.6.

2.4.2 Case Study

The use of case studies within the DSR methodology supports the goal of evaluating the *effectiveness* of a framework's design (Venable, Pries-heje, and Baskerville, 2012). This aligns with the study's goal statement as case studies allow researchers to analyze the application of the framework in its intended real-life environment (Hevner and Chatterjee, 2010). This study uses a holistic multiple case study that involves more than one case but only one unit of analysis (Yin, 1994). It has been decided to limit the study to two cases, primarily due to the time constraints of this study. However, the small number also gives the researcher more time to perform deeper analyses into each case (Gustafsson, 2017). The guidelines for conducting case studies from Runeson and Höst (2009) have been used and are seen in Figure 2.7.

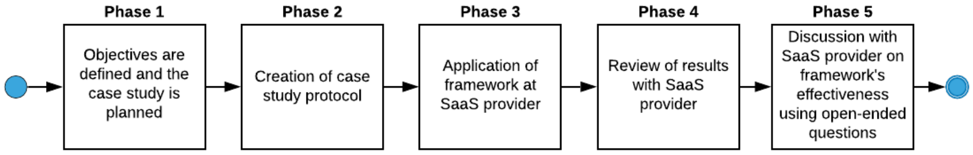

Phase 1
Objectives are defined and the case study is planned
Phase 2
Creation of case study protocol
Phase 3
Application of framework at SaaS provider
Phase 4
Review of results with SaaS provider
Phase 5
Discussion with SaaS provider on framework's effectiveness using open-ended questions

FIGURE 2.7: Case study phases, adapted from Runeson and Höst (2009)

Phase 1 The objective of the case studies is aimed at evaluating the effectiveness of the framework as described in Table 2.4.

Phase 2 To prepare for gathering the data needed to determine effectiveness, a protocol is developed. The protocol contains elements addressing: informed consent, confidentiality, handling of sensitive results, and feedback (Runeson and Höst, 2009). A draft of this protocol is peer-reviewed and piloted before sending it to the prospective SaaS providers. Ensuring that the wording and instructions of the document are clear. Once an agreement has been reached with the provider, the framework is sent to the SaaS provider to allow the provider to gather the required evidence to answer the framework's questions. This is done to reduce the time required to complete phase 3.

Phase 3 Based on the availability of the researcher, a meeting with the SaaS provider is held either in person or online. During this meeting, the framework's questions are addressed with the SaaS provider and, if possible, associated evidence to answer the questions are assessed by the researcher. From this assessment, the appropriate answer inputs are selected, as defined in Section 5.4. Due to limitations in allocated time for each case study, and in the research's ability to assess certain evidence, the SaaS provider is prompted to provide their own answer to the questions.

Phase 4 The results are reviewed and discussed with the SaaS provider, identifying controls have resulted in a weak risk assurance. Additionally, the interactive dashboard is demoed, further demonstrating the reporting abilities of the framework.

Phase 5 The SaaS provider's view of the effectiveness framework is determined by asking open-ended questions using the requirements for a certification scheme seen in Sections 3.10.

Case Study Selection Criteria

Considering the findings of research conducted in the SaaS Continuity Lab by Van Velzen, De Jong, and Jansen (2019), the population of SaaS providers is narrowed to the size of small and medium enterprises (SMEs). European Commision (2003) defines an SME as having a staff headcount of 10 to 250, turnover of €2 million to €50 million or a balance sheet total of €2 million to €43 million. Therefore, the selection criteria are: (1) must provide a Software as a Service; (2) qualify as a SME; and (3) registered as a Dutch company.

Chapter 3

Cloud Ecosystem

3.1 Introduction

Ecosystems do not appear out of thin air, they cultivated and fostered by a set of actors functioning as a unit, within a shared market (Jansen, Cusumano, and Popp, 2019). They are made up of large social, technical, and economic systems, that are multi-leveled, complex, dynamic, adaptive, emergent, and global in nature, containing a multitude of stakeholders motivated by different perspectives and incentives. Jansen and Grance (2011, p. 2) define cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (eg. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or cloud provider interaction." It can be characterized by its on-demand self service, broad network access, resource pooling or multi-tenancy, rapid elasticity and measured service (Ackermann, 2012; Kabbedijk et al., 2014). The National Institute of Standards and Technology (NIST) reported in, Mell and Grance (), the definitions for these characteristics:

- *On-demand self-service:* The ability for an individual to attain cloud services such as storage or computational services through a virtual environment without the assistance of the cloud service provider (CSP).

- *Broad network access:* The ability to connect to the cloud services anywhere with any form of web-enabled device.

- *Resource pooling or multi-tenancy:* The provider's resources are pooled and dynamically allocated based on application demand. Each physical server may have one or multiple tenants via virtual machines.

- *Rapid Elasticity:* This is the ability to scale up, down, or out automatically as workload requirements change.

- *Measured service:* With the above characteristics, the services have the need for metering capabilities capable of monitoring, controlling, and reporting.

Cloud computing at its core is based on the ideas of virtualization and allocation of ICT services across computers worldwide (Sun et al., 2014). Forming the cloud service deployment layers seen in Figure 3.1. Starting with the data centers, the number of services provided to users increases along with the complexity of the situation. The convenience and sharing of resources decrease costs and provides a pay-as-you-go or pay-per-use model, allowing users of all kinds (personal and professional) to adopt the technology along with its benefits and risks (Armburst et al., 2010). Since cloud computing became a popular term in 2007, the cloud has become our source for our entertainment network (Netflix), social network (Facebook), virtual library (as we search on Google for everything), work network (Slack), and development network (Drupal.org) (Bibi, Katsaros, and Bozanis, 2012). This intensive use has created an anticipated worldwide value of cloud computing service to reach €241 billion by the end of 2020 (Khoshkholghi et al., 2014). However, with the onset of the COVID-19 pandemic, the CSPs see massive increases in demand, which will dramatically increase the worldwide value of cloud computing.

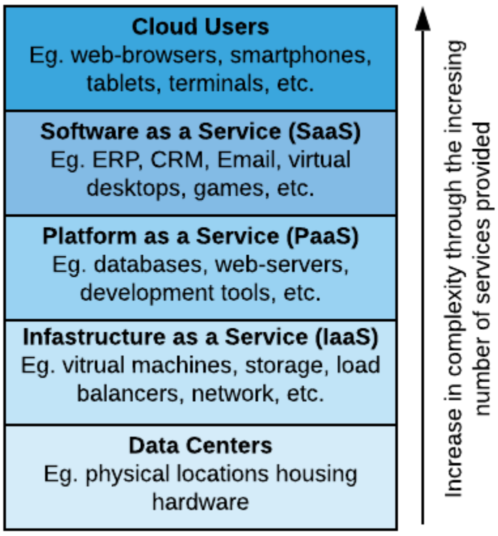

Cloud Users
Eg. web-browsers, smartphones, tablets, terminals, etc.
Software as a Service (SaaS)
Eg. ERP, CRM, Email, virtual desktops, games, etc.
Platform as a Service (PaaS)
Eg. databases, web-servers, development tools, etc.
Infastructure as a Service (IaaS)
Eg. vitrual machines, storage, load balancers, network, etc.
Data Centers
Eg. physical locations housing hardware
Increase in complexity through the incresing number of services provided

FIGURE 3.1: Cloud service deployment layers stack, inspired by Tsai, Sun, and Balasooriya (2010, p. 684)

With all its benefits, the general nature of the cloud gives way to risks that are not easily seen or understood by its end users. Each layer of services can be located at different locations around the world, providing high levels of redundancy. This spreads the risk of disruption in business services by not having all your data in one place (single point of failure risk). However, this makes it more difficult to keep services critical to a user's business operations protected (Arean, 2013). A disruption at any point in the service deployment stack can mean a loss of availability resulting in a user's inability to regain access to their data and application, temporarily or permanently.

3.2 Data centers

Data centers are the backbone of the service deployment stack and are distributed throughout many locations across the globe. These facilities contain servers that house three main physical resources: CPU, memory, and disk, as well as the file system and network data (Birke, Chen, and Smirni, 2012). This hardware and software are actually what the cloud is (Armburst et al., 2010). The cloud comes in four deployment models and is described by Alali and Yeh (2012) as:

- *Public cloud:* Is available to the public or a large industry group and is owned by an organization selling cloud services.

- *Private cloud:* Is a cloud operated solely for an organization by the organization itself or a third party, existing on or off-premise.
- *Community cloud:* Is a cloud that is shared by several organizations and supports a specific community purpose and can be managed by either an organization or a third-party, existing on or off-premise of the community entities.
- *Hybrid cloud:* Is a composition of two or more clouds that remain unique entities but are bound by standardized or proprietary technology that enables data and application portability.

3.3 Infrastructure as a Service

The IaaS layer supplies users with infrastructure resources, such as storage, networking, and processing capacity. Allowing this virtual hardware and operating systems to be controlled through application program interfaces (Catteddu and Hogben, 2009). Making it possible for the IaaS provider to automatically "split, assign, and dynamically resize these resources" (Vaquero et al., 2009). Allowing resources to be allocated as demand for workload capacity fluctuates (Pauley, 2010). Distributing processing and storage services across locations. Creating a cloudiness, that makes it difficult for some users to identify in what servers their data is being processed and stored. An example of an IaaS is *Amazon's* EC2 platform which provides secure, resizable compute capacity in the cloud (Bessemer Venture Partners et al., 2020).

3.4 Platform as a Service

On the PaaS layer, platform solutions are provided through the supported cloud layers. Platforms provide development tools and application programming interfaces for interacting with the platform as well as a run-time environment (Ackermann, 2012). This facilitates software developers' access to a set of services that assist in application design, development, testing, deployment, monitoring, and hosting on the cloud (Tsai, Sun, and Balasooriya, 2010). Requiring no software download or installation and is accessible from anywhere. An example of PaaS is the Google App Engine, which lets developers build scalable web and mobile backends in any language on *Google's* infrastructure (Lomas, 2014).

3.5 Software as a Service

On the SaaS layer, software solutions can be accessed and used through a web-browser, eliminating the need to install the application on a client computer. A SaaS provider manages the operation and maintenance of the application as well as the underlying hardware and software layers (Ackermann, 2012). The SaaS solution and users' data are stored off-premise in a location run by the provider. This places the responsibility of running the ICT support services, including daily software maintenance, data backups, software upgrades, and security on the SaaS provider (Ma, 2007). SaaS typically uses a one-to-many delivery model, referring to the multi-tenancy characteristic allowing one instance of the software to run on a server, accessible by multi-users (Ma, 2007). Therefore, SaaS delivers computing utility, and software. In doing so, the SaaS provider becomes the only one with the ability to get the application back up and running when a disruption occurs in the SaaS supply chain (Hon, Millard, and Walden, 2012). Complicating the situation further, SaaS providers integrate third-party content into their solutions as a means of bolstering the range of services provided (Van De Zande and Jansen, 2011). Resulting in the inability of the SaaS provider to directly restore services, depending on the third-party's ability to restore their services. An example of SaaS is *Netsuite* which is an enterprise resource planning software (Bessemer Venture Partners et al., 2020).

3.6 Cloud Users

Cloud users are individuals who directly use SaaS applications or administrators who configure applications for the end-users (Hogan et al., 2011). Access is granted by the payment of a subscription fees to a SaaS provider, which runs and maintains the software on its own hardware (Mäkilä et al., 2010). Users may or may not be associated with an organization that pays the subscription fees to the SaaS provider.

3.7 Cloud Computing Responsibility

The dividing lines of the four layers in Figure 3.1 are not distinctive. Aspects related to one layer can also be considered to exist in another layer. For example, data storage services can be considered to be either in IaaS or PaaS (Tsai, Sun, and Balasooriya, 2010). Even though Figure 3.1 suggests a hierarchical relationship amongst the different layers, it does not mean that an upper layer has to be built on top of its designated lower layer. For example, a SaaS application can be built directly over IaaS, instead of PaaS (Tsai, Sun, and Balasooriya, 2010). The cloudiness of the ecosystem creates difficulty in assigning responsibility and liability for the services provided.

This is a controversial topic as service providers like *Amazon* take the stance that users and providers should share the responsibilities and risks. Arguing that some service consumers seek the cheapest services while requesting the highest levels of assurances by trying to remove or reduce liability exclusions and limitations, and increase the weight of commitments made in service level agreements (SLA) (Hon, Millard, and Walden, 2012). However, Figure 3.2 displays the level of control of the three main service layers over the cloud technology stack. As the SaaS provider has full control, the responsibility and liability for the security, including continuity, of the services should fall on the SaaS provider (Cloud Security Alliance, 2017b).

This view is supported by the European Union's (EU) General Data Protection Regulation (GDPR), which was initiated in May 2018. The GDPR compliance guide by IT Governance Publishing (2017, p. 11) states, "all data controllers and processors that handle the personal information of EU residents to implement appropriate technical and organizational measures to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services." The main elements of this statement are further defined by IT Governance Publishing (2017) as seen below:

- *Data controller:* The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the

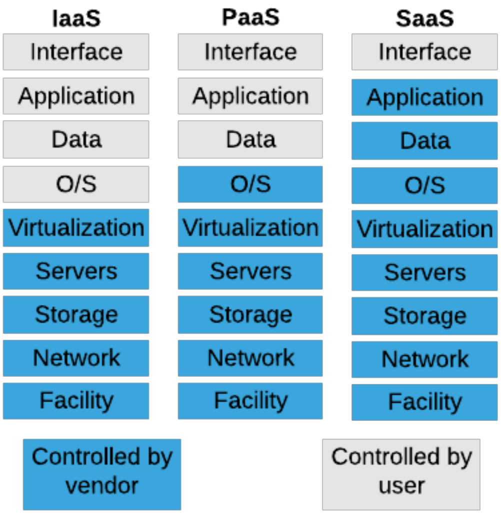


FIGURE 3.2: Cloud layer control over technology stack, inspired by Jansen and Grance (2011, p. 5) and Jayachandran (2014, para. 2)

specific criteria for its nomination may be provided for by Union or Member State law.

- *Data processor:* The natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- *Confidentiality:* The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
- *Integrity:* The property of accuracy and completeness.
- *Availability:* The property of being accessible and usable upon demand by an authorized entity.

The reach of GDPR applies across all EU member states and any organization in the world that provides services to data subjects that are within the EU (IT Governance Publishing, 2017). This coverage means that the diverse storage locations of data do not escape the GDPR's jurisdiction, in theory. The implications of GDPR on cloud computing responsibilities indicate that the SaaS provider should be the only entity in the supply chain to be accessed. It is the view of the researcher, that in addition to GDPR, this answer is the only feasible one as it will be too costly and work intensive to assess every entity in a SaaS supply chain.

3.8 Cloud Computing Risks

Leteinturier et al. (2019, p. 21) describe risk as, "the effect of an uncertainty as to achieving a set of specific objectives." The risks involved in cloud computing can seem to be endless due to the complex nature of the cloud ecosystem. As this study aims at covering a broad range of relevant risk topics, it is necessary to fine-tune the scope by seeking ranked cloud computing risk lists that provided guidance into which are the major risks. During the MLR, it became evident that the majority of research focused on the area of data security as a component of cloud computing risks.

Notably, the researcher noticed differing use of terminology used in cloud computing differed throughout academic and grey literature. Potentially leading to misunderstanding of what certain author's are referring to. Dutta, Peng, and Choudhary (2013) also encountered this when developing their enterprise cloud computing ontology. The ontology in Dutta, Peng, and Choudhary (2013) is adopted to provide a scientifically grounded foundation for categorizing risks. Figure 3.3 displays a modified version of the ontology suited to this study.

The original ontology has been broken into four high-level categories and twelve sub-categories. The main categories being *Organisational risks*, *Operational risks*, *Technical risks* and *Legal risks*. Sub-categories of this ontology that cover only the internal operations of the SaaS customer, and do not pertain to the SaaS customer's ability to safe guard and access their data or SaaS solution are removed, Ensuring only relevant topics to this study's aim are considered. Some modifications to the wording of the sub-categories are made to improve understandability and the sub-categories of *SaaS continuity guarantee* and *Financial Stability* are added to enrich the ontology for this study. Notably, the *Standards Compliance* sub-category is investigated with the intent to identify design requirements from existing standards and frameworks applicable to ICT and business continuity. This is discussed in Sections 3.9 and 3.10.

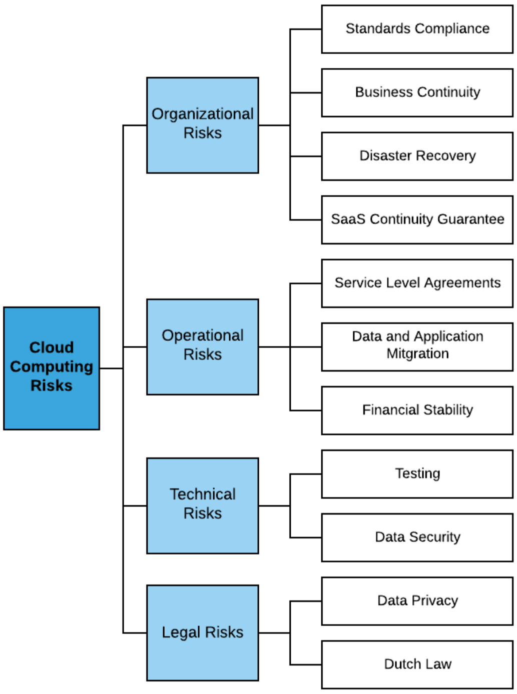


FIGURE 3.3: Modified cloud computing risks ontology, adapted from Dutta, Peng, and Choudhary (2013, p. 5)

The goal of Dutta, Peng, and Choudhary (2013, p. 39) is to "explore potential risks that organisations may encounter during cloud computing adoption, as well as to assess and prioritise these risks, from the perspective of ICT practitioners and consultants". The ontology is used in conjunction with a questionnaire to extract views on the risks from 39 ICT experts from around the world. The feedback is then used to rank the risks. The risks involved in cloud computing can seem to be endless due to the complex nature of the cloud ecosystem. As this study aims at covering a broad range of relevant risk topics, it is necessary to fine tune the scope by seeking ranked cloud computing risk lists that provided guidance into which are the major risks seen in Table 3.1.

TABLE 3.1: Modified list of cloud computing adoption risks from Dutta, Peng, and Choudhary (2013) and Armburst et al. (2010)

Risk Ranking	**Armburst et al. (2010)**	**Dutta, Peng, and Choudhary (2013)**	**Palos-Sanchez (2017) (data is from 2014)**	**Al-Hujran et al. (2018)**
1st	Availability/ business continuity.	Privacy of enterprise or customer data is jeopardised in the cloud.	Risk of a security breach.	Security concerns.
2nd	Vendor lock-in.	Inconsistent data protection laws adopted by different countries where cloud data are generated and stored.	Uncertainty regarding applicable legislation, jurisdiction and the mechanism for resolving disputes.	Reliability.
3rd	Data confidentiality and auditability	Difficult for user companies to change cloud vendors even in the case of service dissatisfaction (also known as vendor lock-in).	Uncertainty about the location of the data.	Privacy concerns.
4th	Data transfer bottlenecks.	User companies lack disaster recovery and contingency plans to deal with unexpected technical issues in cloud environment.	Problems accessing the software or the data.	Loss of control.
5th	Performance unpredictability.	Enterprise data migration difficulties at the end of the cloud contract.	Difficulties with leaving or changing CSPs.	Vendor lock-in.

The literature selected are based on the following criteria: (1) must not focus on one specific aspect of cloud computing; and (2) must be published scientific literature. An attempt is also made to use literature from different dates to identify any long-lasting risks. The literature selected are displayed in Table 3.1. It shows the top five risks from Armburst et al. (2010), Dutta, Peng, and Choudhary (2013), Palos-Sanchez (2017), and Al-Hujran et al. (2018). It must be noted that Al-Hujran et al. (2018) did not rank the topics but as it is a systematic literature review, the count of literature supporting each topic is used to rank them in this study. By grouping similar risks listed in Table 3.1, important areas of research for this study emerged. Using the sub-categories of Dutta, Peng, and Choudhary (2013)'s ontology to guide the grouping of topics. The following groups are identified: business continuity, disaster recovery, data security, data privacy, and data and application moveability. The grouping activity also attempted to reduce the overlap of the topics as much as possible. These topics are discussed in Chapter 4 along with other topics that fall within the groups.

3.9 ICT & Business Continuity Standards

Cloud Computing, as we know of it today is a young information and communication technology (ICT) industry that not yet been fully standardized (Moravcik, Segec, and Kontsek, 2018). Luckily, many existing ICT industry standards are applicable to the cloud domain. The organizations that create these standards can be placed in two groups. The first group focuses mainly on aspects of technology, and the second deals with business standardization. However, the context of this study requires a blend of business and technology aspects to be included in the framework.

Diving deeper into the grouping of standards, Baudoin et al. (2016) distinguishes between three types of cloud standards seen below:

- *Advisory standards:* These are aimed at being flexible enough to be interpreted and applied to all types of organizations. Allowing them to make use of controls that are applicable to them. However, these characteristics make it unsuitable for straightforward compliance testing used by most certification schemes.
- *Security frameworks:* These frameworks define specific policies, controls, checklists, and procedures along with processes for supporting that auditors to assess and measure a CSP's compliance. These types of standards are suitable for certification.
- *Standards specifications:* These types of security standards specifically define application program interface, data structures and communication protocols that must be implemented to claim support for the standard.

Based on these definitions, this study aims to create a framework that qualifies as a security framework as it is suitable for awarding certification marks. Certification of cloud services can cope with the challenging lack of transparency, trust, acceptance, and play an essential role in the dissemination of technologies, knowledge and, as such, contribute to a nation's gross domestic product (Sunyaev and Schneider, 2013; Habil et al., 2018).

This positive impact of certifications is also visible in the business continuity industry from *Business Continuity Institute's (BCI)* Horizon Scan Report 2020. The report displays the results from a survey on the current stats of the business continuity industry trends, consisting of 665 respondents across 74 countries. Figure 3.4, displays the responses to the question, "What benefits does certification provide to you and your organization?" Providing insights into the levels of impact that a business continuity certification can have on a number of business aspects. As business continuity is a major focus of this study's framework, this data provides an indication of the potential value arising from the application of this framework and similar artefacts.

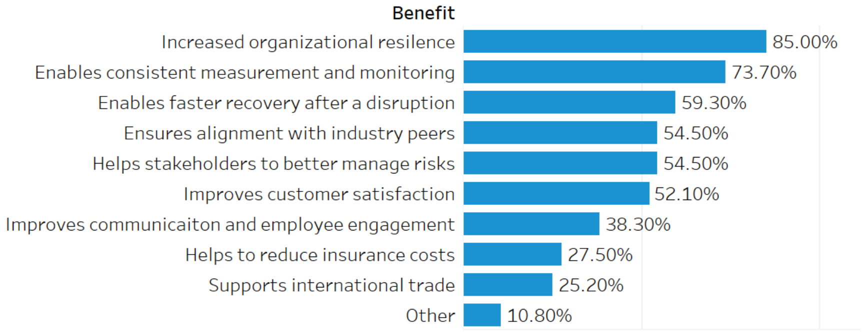


FIGURE 3.4: Business continuity certification benefits, extracted from Elliott, Thomas, and Muhammad (2020, p. 32)

3.9.1 Standards Landscape

By untangling the jungle of standards that are relevant to this study, the knowledge base for developing requirements for the design of the framework. Additionally, this list of standards provides the user of the SaaS continuity control framework with the ability to identify existing standards that may satisfy the questions posed by the framework. The *European Commission's Unit on Software and Services*, funded an initiative called *CloudWATCH2*. It is a European cloud observatory mission supporting cloud policies, standard profiles, and services (CloudWatch2, 2017). The initiative ended in August 2017, but released a guide on standards relating to the cloud. *CloudWATCH2* breaks the standards into three groups: portability, interoperability, and security (CloudWatch2, 2017). Hogan et al. (2011) describes these groups as seen below:

- *Portability:* Refers to the movement of data from one cloud system to another and the ability of applications to be ported and run on different cloud systems at an acceptable cost.
- *Interoperability:* Refers to the management and functional interfaces of cloud services between cloud consumer applications and cloud service, and between CSPs themselves.
- *Security:* Refers to the objectives of ensuring the confidentiality, integrity, and availability of information and information systems.

Combining the findings from the MLR and standards lists from CloudWatch2 (2017), Elliott, Thomas, and Muhammad (2020), and Kosutic (2015), Appendix C.1 displays the standards and frameworks associated with each previously defined group. Of the items listed, focus is made on the *Cloud Controls Matrix v3.0.1* (Cloud Secuirty Alliance, 2014). It becomes the benchmark for the SaaS continuity framework, as it is composed of 310 questions across 133 security controls, grouped into 16 cloud technology related domains. It is freely accessible and contains an extensive matrix of cloud-specific security controls, mapped to leading standards, best practices and regulations. This matrix is used as a benchmark for the certification framework's design decisions. Notably, standards associated with business continuity are included in the security section of Appendix C.1. This is justified following (IT Governance Publishing, 2017)'s definition of availability; a measure of being accessible and usable upon demand by an authorized entity, and ISO (2019)'s definition of business continuity; the capability of an organization to continue the delivery of products and services during a disruption. The researcher argues that business continuity can be directly associated with the measure of the availability of services within the cloud ecosystem. If a CSP fails to implement a business continuity plan, it can be assumed that the potential for the provided cloud services to go become unavailable increases.

3.10 ENISA Cloud Service Provider Certification Scheme

The *European Union Agency for Cybersecurity (ENISA)* developed the *Cloud Service Provider Certification* scheme. This scheme is a guide for cybersecurity certification of ICT services, products and processes, including cloud services. The development of the *Cloud Service Provider Certification* scheme was initiated by Regulation (EU) 2019/881 (European Union Cybersecurity Act) (Leteinturier et al., 2019; Tajani and

Ciamba, 2019). Barreira et al. (2019) provide insight into article 51 of the *European Union Cybersecurity Act* states that any European cybersecurity certification scheme should be designed with the following security objectives in mind:

- To protect stored, transmitted or otherwise processed data against accidental or unauthorised destruction, loss or alteration or lack of availability during the entire life cycle of the ICT product, ICT service or ICT process.
- That authorised persons, programs or machines are able only to access the data, services or functions to which their access rights refer; to identify and document known dependencies and vulnerabilities.
- To record which data, services or functions have been accessed, used or otherwise processed, at what times and by whom.
- To make it possible to check which data, services or functions have been accessed, used or otherwise processed, at what times and by whom.
- To verify that ICT products, ICT services and ICT processes do not contain known vulnerabilities.
- To restore the availability and access to data, services and functions in a timely manner in the event of a physical or technical incident.
- That ICT products, ICT services and ICT processes are secure by default and by design that ICT products, ICT services and ICT processes are provided with up-to-date software and hardware that do not contain publicly known vulnerabilities, and are provided with mechanisms for secure updates.

These objectives provide a set of requirements for the development of this study's framework. Article 54 presents additional core requirements that need to be present in a certification scheme(Barreira et al., 2019). However, the majority of these elements are concerned with long term outcomes (refer to Figure 2.5) of the framework and is outside the scope of this study . Article 52 of *European Union Cybersecurity Act* describes the assurance levels for a scheme and explains how these should be specified. Article 52 results in three assurance levels that a certification can achieve:

- *Basic:* Aims to minimise the known basic risks for cyber incidents (disruptive events) and cyber attacks.
- *Substantial:* Aims to minimise known cyber risks, cyber incidents (disruptive events) and cyber attacks carried out by actors with limited skills and resources.
- *High:* Aims to minimise the risk of state-of-the-art cyber attacks carried out by actors with significant skills and resources.

Future development of this framework can use the *Cloud Service Provider Certification* scheme as a guide to achieve EU recognized assurance level. Table 3.2 shows the assurance level achieved by existing certification organizations. In an attempt to create a framework that may one day make this table, the researcher has attempted to adhere to some of the elements present in the *Cloud Service Provider Certification* scheme.

TABLE 3.2: Existing cloud specific certifications and achieved assurance level, extracted from Barreira et al. (2019)

Assurance Level	Cloud Certification	Cloud Service Layer
Basic	Trusted Cloud	IaaS, SaaS
	Zeker Online	Infrastructure
	ENS low	IaaS, SaaS
Substantial	BSI C5	IaaS, SaaS
	CSA STAR	IaaS, SaaS
	ISO 27017	IaaS
	ENS medium	IaaS, SaaS
High	SecNum Cloud	IaaS, SaaS
	ENS high	IaaS, SaaS

In the future, this study's framework may aim to achieve the basic assurance level recognition. Thus attention is brought to Barreira et al. (2019, p. 24)'s view and recommendation on self-assessment certification schemes: "Due to the complexity of the cloud computing supply chain, as well as the criticality of the data and applications deployed on a cloud service, a security breach can have severe consequences for the cloud user and the application provider (eg. SaaS). Therefore, self-certification shall not be accepted in the basic level of assurance."

3.11 Takeaways

Within this chapter, the major concepts of the cloud ecosystem have been discussed to ensure that the study's understanding of the ecosystem is sound. Within this ecosystem, the top risk concepts have been identified and added to the knowledge base to strengthen the DSR cycle. Leading to a more targeted approach in the literature study's aim to extract requirements for the framework. Such findings have prompted updates to be made to the conceptual model previously seen in Figure 1.1, creating version 2 which is displayed in Figure 3.5. The contributing concepts extracted from this chapter are listed:

- The study's point of view has been developed on which entity should be responsible for the continuity of a SaaS solution, and assessed using the framework.
- Top cloud computing risks have been identified in Figure 3.3, and used to identify the high-level domains that become the main research concepts in the following chapter 4.
- The study's artefact has been classified as a security framework providing a better indication of the role the framework plays in the ICT security domain.
- The elicitation of *ENISA* certification scheme requirements in Section 3.10 is used in the case study phase to determine the framework's degree of **effectiveness** as a security certification framework, and alignment with *ENISA's* security objectives.

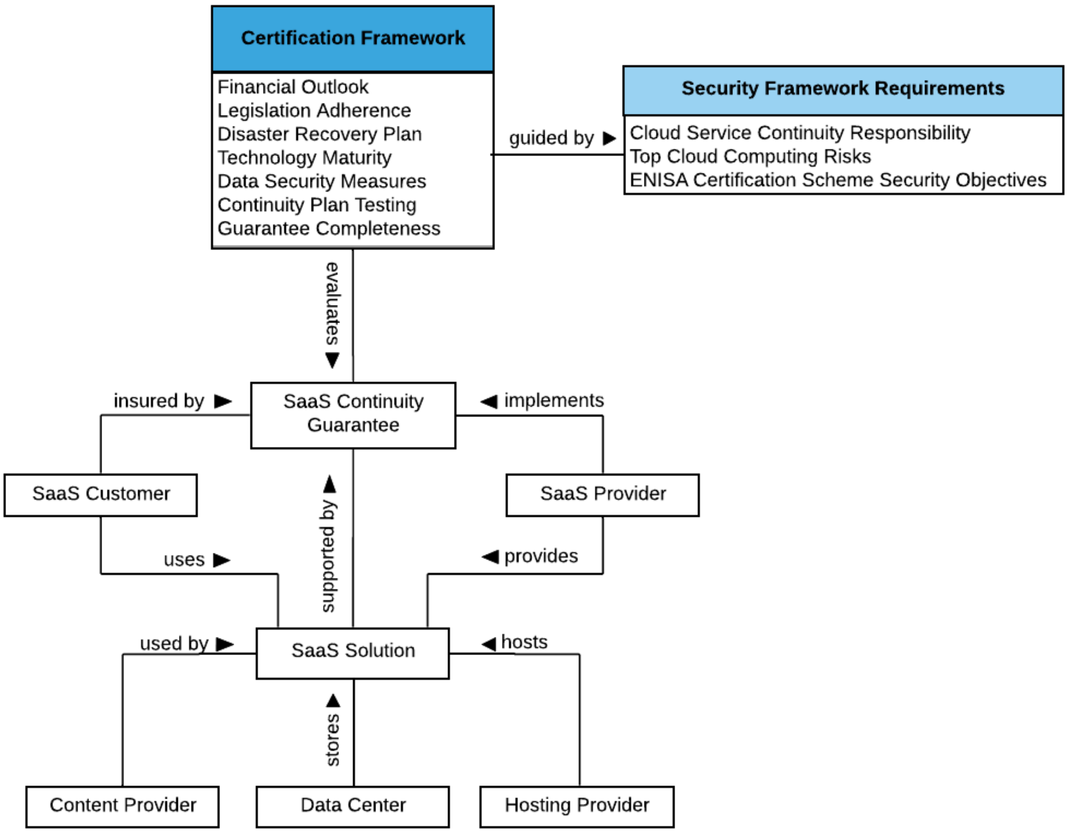


FIGURE 3.5: Research context conceptual-model version 2

Chapter 4

SaaS Risks

4.1 Introduction

This chapter serves as an investigation into the concepts displayed in the modified risk ontology displayed in Figure 3.3. The investigation aims to extrapolate security framework requirements from the literature found on each concept. Tables and lists have been used to provide enhanced clarity on the requirements that are included in the first draft of the framework. Additionally, relevant statistics are provided to enrich the chapter with evidence of the relevance and real-world impact of the topics discussed. Figure 4.1 displays the structure of the chapter, as well as the concepts and sub-concepts discussed. Noticeably, some concepts contain few or no sub-concepts, resulting from scoping decisions based on the depth of the information pool relevant for this study, and the required granularity of the information for use in the framework. Specific mention is brought to *data security*, this concept is vital and complex, and can arguably form its own framework. For this reason, it has been scoped to remain at a low-level of granularity.

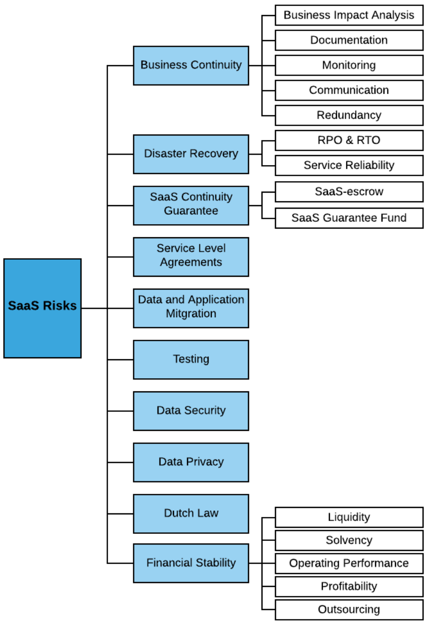


FIGURE 4.1: SaaS risk concepts examined in Chapter 4

4.2 Business Continuity

As previously stated, business continuity enables an organization to continue delivering products and services within an acceptable time frame during a disruption event (ISO, 2019). This capability is supported by an organization's business continuity plan. The differences between business continuity and disaster recovery are sometimes blurred, and the terms are used interchangeably throughout literature. Therefore, this study views business continuity as an umbrella term that covers developing, testing, and managing enterprise-wide business continuity plans, while disaster recovery is focused on developing continuity capabilities for business-critical information and communication technology (ICT) infrastructure and applications (Audit and Association, 2012; Alshammari, Alwan, and Alshaikhli, 2016). A business continuity plan is proactive and indicates what people, processes, and technology are required to continue operations when a disruption occurs (CompTIA, 2019). It stipulates the wait time in a disruption event before the disaster recovery plan initiates (Arean, 2013). This time can be set in service level agreements (SLA) detailing the minimum availability and response time, however there are many factors that need to be considered when creating a business continuity plan (Catteddu and Hogben, 2009). In Elliott, Thomas, and Muhammad (2020), the unnamed Head of Business Continuity Management & Technology, in the United Kingdom is quoted:

> As we continue to move forward with new technology solutions, we are growing our reliance more and more on third-party software. When new technology such as software as a service (SaaS) is implemented, there are different pros and cons from business continuity risk management perspectives. If sufficient due diligence is not conducted regularly, then the probability of an unexpected disruption would certainly increase and more when the organization is undergoing technological change.

Business continuity plan and disaster recovery plan are two overarching facets of business continuity management and include elements such as, risk assessment, business impact analysis, risk mitigation, and contingency planning (Stanton, 2005). Wiboonrat and Kosavisutte (2008) state that business continuity management should be aimed at emphasizing the importance of:

- Understanding business continuity needs and the necessities for establishing policies and objectives for business continuity.
- Implementing and operating controls for managing overall business continuity risks.
- Monitoring and reviewing the performance and effectiveness of the continuity system.
- Continuous improvement based on objective measurement.

When addressing these areas, organizations must identify a set of strategies that take into consideration the resources available to achieve set objectives (Alhazmi and Malaiya, 2013). When setting objectives, the organization's staff, technologies, and monetary strength must be identified to ensure that objectives are achievable.

4.2.1 Business Impact Analysis

To create an effective business continuity plan, a business impact analysis should be conducted to identify critical business functions, resources needed to continue operations when a disruption event occurs, and assess the risks to business functions (CompTIA, 2019). Critical functions are the functions that are needed to provide key services that allow operations to continue (Torabi, Rezaei Soufi, and Sahebjamnia, 2014). Torabi, Rezaei Soufi, and Sahebjamnia (2014) provide a set of measures for determining the critically business functions:

- *Recovery time:* The time needed to return a business function to its usual state.
- *Recovery cost:* Cost of operations for returning a business function to its usual state.
- *Possibility of outsourcing function:* Existence of companies to outsource a business function.
- *Importance:* Business functions have different roles in supporting services, and some can be completed at any time while some require completion at a specific time.
- *Required manpower for recovery:* Manpower needed for returning a business function to its usual state.
- *Vulnerability:* Degree of influencing of a business function from disruption events.

A risk can be seen as any reasonably identifiable circumstance or event that has the potential to negatively impact business operations (Leteinturier et al., 2019). CompTIA (2019, p. 3) describes a risk assessment as, "the systematic process of studying the areas of potential risk to corporate operations." A risk assessment should identify risk controls, risk severity levels according to probability of occurrence, and impact on the business (CompTIA, 2019; Cerullo and Cerullo, 2004; Wiboonrat and Kosavisutte, 2008). Risks have differing levels of impact on the SaaS provider with different effects. This requires the risks to be weighted differently in order to provide an accurate score of the SaaS provider's risk mitigation measures. Barreira et al. (2019) state that a risk assessment process is commonly composed of the five steps below:

1. *Establishment of a risk assessment framework:* Create or adopt a risk assessment tool.
2. *Identification of risks:* Determine what are the threats that need to be analyzed.
3. *Analysis of risks:* Define requirements for achieving a satisfactory risk assurance level accounting for the benefits versus cost, risk probability, and risk impact levels.
4. *Evaluation of risks:* Based on the requirements, assign a risk severity level.
5. *Selection of risk management option:* Based on the risks and their severity level, determine appropriate actions need to mitigate and react to risk occurrence incidents.

To complete the risk evaluation step, a risk evaluation matrix can be implemented by an organization (Leteinturier et al., 2019). This matrix evaluates a risk's severity based on its probability and impact. As each SaaS solution's architecture will differ, the risk severity levels may vary significantly with the cloud architecture being used (Catteddu and Hogben, 2009). The use of a risk evaluation matrix can be seen in Elliott, Thomas, and Muhammad (2020). There is no specific mention of which risk evaluation matrix is used in this *BCI* report. However, viewing Figure 4.2, one can see the use of risk impact and probability previously mentioned.

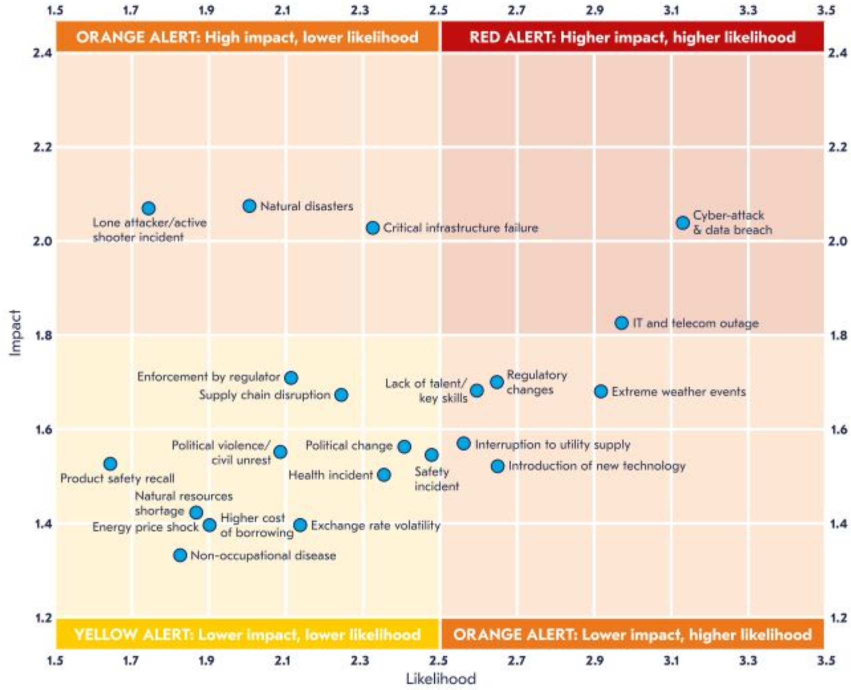


FIGURE 4.2: Risk evaluation forecast for 2020, extracted from Elliott, Thomas, and Muhammad (2020, p. 21)

Publishing of Elliott, Thomas, and Muhammad (2020) occurred during the early stages of the COVID-19 outbreak, and does not reflect the impact of the pandemic. COVID-19 can be classified under *Non-occupational disease* which is ranked second from last in Elliott, Thomas, and Muhammad (2020)'s list of forecasted threats. In Elliott, Thomas, and Muhammad (2020, p. 1), the chair of *BCI*, reflected on this addressing the unpredictability of risks, "[Non-occupational disease's] lowly position in the 2020 results illustrates how, while the world's attention is elsewhere, a different threat can suddenly erupt and cause significant disruption." The high ranking of *cyber attack and data breach*, may increase as the global disruption caused by COVID-19 continues to reveal countless vulnerabilities of ICT systems worldwide. This is can be seen in the surges of reports in ransomware and other attacks in the health industry, specifically hospitals and research entities tackling COVID-19 (Newman, 2020).

4.2.2 Documentation

Information system and business continuity plan documentation (eg. administrator and user guides, architecture diagrams, and assigned roles and responsibilities) shall be made available to authorized personnel to ensure the configuring, installing, and operating of the SaaS system is done effectively (Shanthan, 2016). Just as testing is done periodically, the documentation should be evaluated by management periodically and updated as changes occur (Zeker-Online, 2019). Reports and logs of disruption events and resulting downtime should also be accessible (Rutherford, 2019).

4.2.3 Monitoring

A suitable method for the monitoring of service levels, information security, compliance with relevant legislation and regulations, and staff training are the only ways management can ensure that the business continuity plan can be effectively executed (Jeon and Seo, 2015; IT Governance Publishing, 2017). Real-time monitoring enables an organization to assign severity levels to disruption events and determine the correct course of action (Catteddu and Hogben, 2009). Without this, affected entities can not be informed of the disruption in a timely manner. This extends to third-party service providers as they need to demonstrate compliance with information confidentiality, integrity, and availability, access control, service definitions, and SLAs stipulated in their contracts (Cloud Security Alliance, 2017a). Cloud-based disaster recovery systems simplify the situation with the ability to monitor primary data centers, making it easier to differentiate a simple network failure from a disaster situation and react accordingly (Saquib et al., 2013).

4.2.4 Communication

In order for a business continuity plan to be effective, coordination between staff must take place through specified communication channels (Zeker-Online, 2019). It is also essential to establish an external communication plan (eg. supply chain entities and customers) (CompTIA, 2019). A key component is the ability to quickly identify assigned personnel that responsible for communicating disruption status updates to employees and being the organization's spokesperson towards the public (Cloud Security Alliance, 2017a). Public communication plays an important role as providers may make modifications to the terms of service (eg. posting an updated version online) without giving any direct notification to the consumer (Alali and Yeh, 2012).

4.2.5 Redundancy

Data redundancy is needed for preventing data loss and achieving set fault-tolerance levels in cloud computing (Wang et al., 2013). There should be multiple paths to the same set of systems so that a problem in a single path can occur with little or no disruption to other paths. A fail over plan supports this switch over from primary equipment to secondary equipment (CompTIA, 2019). Redundancy does not only include networking, servers, and disk storage. A SaaS provider should identify secondary vendors who can provide services if the primary vendor is unable to deliver (Cloud Security Alliance, 2017a). The hybrid cloud model supports these needs as it enables data and application portability (Alali and Yeh, 2012).

4.3 Disaster Recovery

Disaster recovery, aims at developing stand-alone databases and application systems allowing operations to quickly come back online after experiencing a severe disruption. They must be able to temporarily replace the host system and handle operations' workload when the host system is unable to function (Alshammari, Alwan, and Alshaikhli, 2016). This is possible due to the rapid elasticity of the cloud and its pay-per-use pricing model. Allowing a SaaS provider to acquire resources needed for operations, such as data storage and applications, from third-party entities (Saquib et al., 2013). Disaster recovery plans need to account for fault tolerance, which is the system's ability to withstand sudden changes due to any type of failure, and is measured with recovery point objectives (RPO) and recovery time objectives (RTO) (Mesbahi, Rahmani, and Hosseinzadeh, 2018). Additionally, the handling of financial costs associated with data transfers, storage, third-party hosting, such as SaaS-escrow, and the cost of downtime must be accounted for (The Cloud Service Measurement Initiative Consortium (CSMIC), 2014).

Downtime costs can result in massive revenue loss and may even cause an inevitable shutdown in the future. Table 4.1 shows the potential severity of downtime costs, despite a company having high service availability. Notably Gagnaire et al. (2012), acknowledge that the costs used to create Table 4.1 vary tremendously in reality.

TABLE 4.1: CSP downtime costs, sourced from Gagnaire et al. (2012)

Cloud Service Provider	**2013 Downtime (Hours)**	**Availability (%)**	**Cost (€)/ Hour**	**Total Cost (€)**
Microsoft Azure	272.04	96.89	309,120	84,093,004
IBM	223	97.45	309,120	72,024,960
Amazon Web Service	68.18	99.67	309,120	21,075,801
Salesforce	84.72	99.03	184,000	15,588,480
Dropbox	17	99.80	184,000	3,128,000

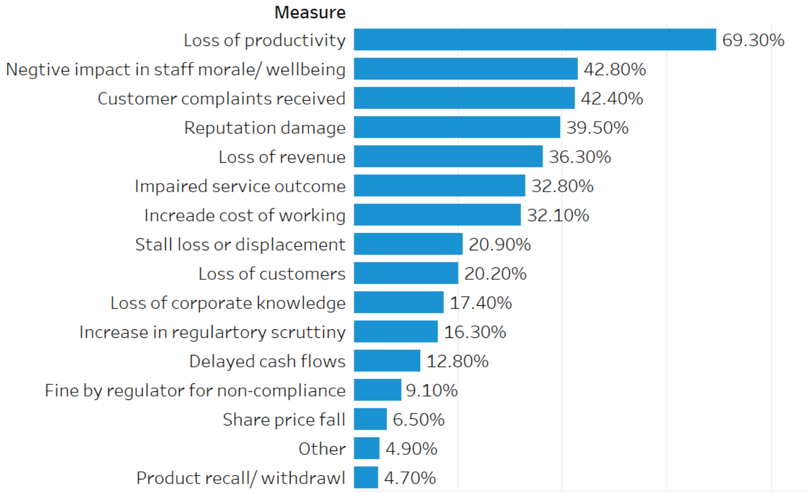


FIGURE 4.3: Measures of impact from disruption events in 2019, extracted from Elliott, Thomas, and Muhammad (2020, p. 24)

Excluding financial costs, there are many other measures that are negatively impacted by disruption events. Elliott, Thomas, and Muhammad (2020), provide a list of areas that are impacted, seen in Figure 4.3. The top four impacted areas in Figure 4.3 are non-tangible, in the area of internal/ external human responses to disruption events. Suggesting the further development of this study's framework should include a domain on human resources. This is not covered in this study, as the focus is applied more on the business technological aspect of the study's context.

4.3.1 Back-up Strategy

There are three options for back-up strategies that support an organization's disaster recovery plan, namely, cold, warm, and hot strategies (Suguna and Suhasini, 2014). Cold back-ups often only replicate data on a periodic basis resulting in an RPO of hours to days. Additionally, it requires additional preparation time to get servers ready to run the application resulting in a high RTO (Sabbaghi, Mahboubi, and Othman, 2017). The only advantage to a cold back-up is its low costs. The next back-up strategy is warm, which has standby servers available to run the application after a failure occurs, taking minutes to become available (Sabbaghi, Mahboubi, and Othman, 2017). A hot back-up strategy uses synchronous replication to prevent data loss by means of a set of mirrored stand-by servers that are always available to run an application (Suguna and Suhasini, 2014; Sabbaghi, Mahboubi, and Othman, 2017). This strategy is needed for business-critical applications and is the most effective strategy and costly of the three. Figure 4.4 provides a visual of a hot back-up site situation.

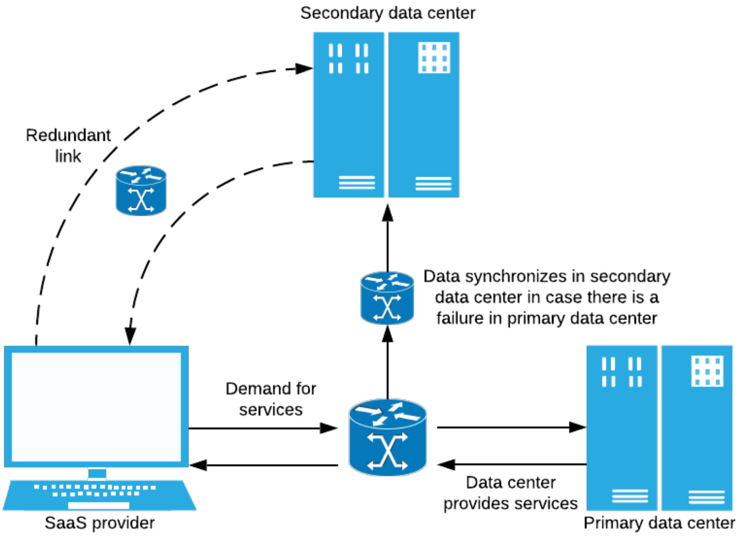

Secondary data center
Redundant link
Data synchronizes in secondary data center in case there is a failure in primary data center
Demand for services
Data center provides services
SaaS provider
Primary data center

FIGURE 4.4: Hot back-up site situation, adapted from Sabbaghi, Mahboubi, and Othman (2017)

4.3.2 RPO & RTO

When systems encounter failures to its primary resources, a failover plan is initiated, switching the system over to a back-up system (Suguna and Suhasini, 2014). Whereas, a failback plan is the switch from the back-up system to the primary system when failures in the primary system have been rectified. These plans have a cost and need to have an allocated budget that addresses RPOs and RTOs. RPO quantifies the acceptable amount of data that can be lost, and RTO the acceptable outage time for a business process or application (Wiboonrat and Kosavisutte, 2008). RPO values range from a few minutes to several hours, whereas RTO values range from a few minutes to a few days (Alhazmi and Malaiya, 2013). RPO can be interpreted as the highest allowable time between back-ups (Alshammari, Alwan, and Alshaikhli, 2016). The lower the RPO, the higher the total expense of preserving the required infrastructure needed to support recovery efforts. The timeline and positioning of RPO, RTO, and data-backups in a disaster recovery plan is shown in Figure 4.5. *T1 - T6* represent the time to complete each activity, adding up to the total RTO.

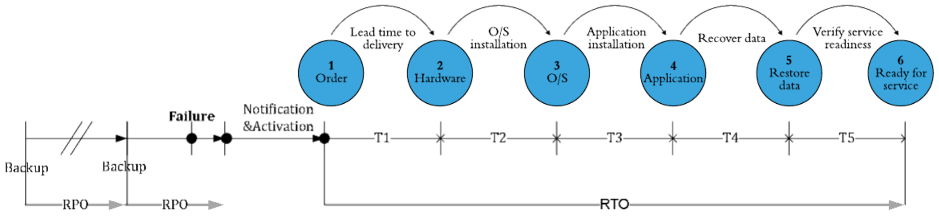


FIGURE 4.5: Recovery point objective (RPO) and recovery time objective (RTO) time line, extracted from Wiboonrat and Kosavisutte (2008, p. 679)

4.3.3 Service Reliability

The reliability of a service is the correctness of its responses according to its specifications, and should not be confused with availability, which is the system's ability to respond (Dudouet, Edmonds, and Erne, 2015). Due to cloud computing's resource pooling characteristic, failure at one of the entities involved in the supply chain is inevitable. For this reason, reliability in cloud computing is measured using mean time till recovery, which is the average time it takes to get a service up and running again after a failure (Adams et al., 2014). There are a few types of failures that need to be measured. Kaur and Kumar (2015) provides a list of these failure types:

- *Overflow:* When the job request queue reaches its limit and users are unable to get the service they want after the maximum number of new requests have been discarded.
- *Timeout:* This occurs when the set waiting time for a requested job to be completed is surpassed.
- *Data resource missing:* When data resources registered on the data resource manager are removed but the data resource manager is not updated. This results in any job request for that data resource to fail.
- *Computing resource missing:* When a computing resource (physical or virtual) is unavailable, any request for that resource will fail.
- *Software failure:* This failure is due faults or unexpected results in active programs.
- *Database failure:* When a database crashes and all requests to access fail.

- *Hardware failure:* When the physical components of the computing resources or data resources stop working.

In order to shrink mean time till recovery, a SaaS provider needs to implement design, development, and training practices that improve detection and recovery from the different types of failures. By following the design principles by Adams et al. (2014), a SaaS provider can shrink the mean time till recovery by apply:

- *Design for resilience:* The service must withstand component-level failures without requiring human intervention, be able to detect failures, and automatically take corrective measures. When failure occurs, the service should degrade smoothly, providing partial functionality rather than abruptly going offline.
- *Design for data integrity:* The service must capture, manipulate, store, or discard data in the correct manner according to set specifications.
- *Design for recoverability:* A service or its components should be able to recover quickly and automatically and the teams should be able to restore services quickly and completely if disruption occurs.

These design areas can be addressed by seeking compliance with the appropriate standard specifications. Compliance with such specifications can reduce the number of software imperfections, human errors, and infrastructure failures. Ideally, these specifications should influence the development services at the early stages of the software development life-cycle.

4.4 SaaS Continuity Guarantee

A SaaS continuity guarantee is a type of insurance offered by a SaaS provider to a SaaS customer, that stipulates the details about the availability of data and services in the event of a disruption in the SaaS supply chain (Cerullo and Cerullo, 2004; Van De Zande and Jansen, 2011; Snedaker and Rima, 2013). Van De Zande and Jansen (2011) list the requirements for a complete SaaS continuity guarantee as (in order of importance):

1. *Own Backup:* Every SaaS customer should be able to download all of its data.
2. *Hosting Insurance:* A third-party should create an arrangement with the hosting provider to continue hosting even if the SaaS provider fails.
3. *Arrangement with content providers:* If the SaaS application contains paid content from third-parties, they should also continue providing the content.
4. *Support and maintenance for the application:* If the SaaS provider disappears, the customer also loses support. A third party could try to continue support for the application.

It is essential that a SaaS customer ensures that these topics (at a minimum) are covered in the terms and conditions for a cloud service agreement. Two types of service agreements exist, non-negotiable agreements and negotiated agreements. Non-negotiable agreements create the economies of scale enjoyed by public cloud computing that is necessary for its survival (Alali and Yeh, 2012). SaaS providers tend to lean towards excluding liability clauses in their agreements, particularly for outages and data loss (Hon, Millard, and Walden, 2012). *Iron Mountain*, an enterprise information management company, reported in their article Boruvka (2016), that 79% of SaaS providers do not guarantee application continuity. Providers justify this lack of liability, stating that they already provide a commoditized service and that customers should bear the burden of risk (De Jong, Jansen, and Overbeek, 2019). Hon, Millard, and Walden (2012, p.94) state that this is understandable, as "providers may not wish to be exposed to say 100 million of liability for a deal worth 1 million; and unlimited liability could put smaller providers out of business."

Liability agreements are usually coverage across multiple documents, such as SLAs, privacy policies, acceptable use policies, and terms of use (Alali and Yeh, 2012). Alali and Yeh (2012) describes these documents as follows:

- *SLA:* Represents the understanding between the cloud consumer and cloud provider about the expected level of service to be delivered. Elements covered in SLA can be used as triggers for business continuity plans or disaster recovery plans, and should be considered even though an SLA does not meet the requirements of a SaaS continuity guarantee.
- *Privacy policy:* Documents information handling practices and how consumer information is collected, used, and managed.
- *Acceptable use policy:* Identifies prohibited behaviors by cloud consumers.
- *Terms of use:* The licensing of services, limitations on liability, and modifications to the terms of the agreement.

Privacy and security risks are dependent on these agreements. In this study, only SLAs are explored as they typically contain quantifiable elements that can be directly linked with mechanisms for maintaining service availability, which is also the aim of implementing SaaS continuity guarantees (Ackermann, 2012).

4.4.1 SaaS-escrow

Before SaaS-escrow, there was software escrow, which is a service that helps protect all parties involved in a software license by having a neutral third-party escrow agent hold source code, data, and documentation until a trigger event occurs (Weigl, Binder, and Strodl, 2013). SaaS-escrow is a modified version of the regular source-code or software escrow that can contain additional features such as, data back-ups, the deposit of source-code, and the continuation of SaaS solution hosting through a third-party hosting provider (Van De Zande and Jansen, 2011). A visual of the SaaS-escrow situation is given in Figure 4.6.

Escrows have two main types, single beneficiary, and multiple beneficiary. A single beneficiary arrangement is between the SaaS provider, one SaaS customer and the escrow agent, where as a multiple beneficiary arrangement contains multiple SaaS customers. In single beneficiary arrangements, the SaaS-escrow is typically more negotiable than in a multiple beneficiary situation, as a standardized master contract is typically applied to the beneficiaries (EscrowTech, n.d.). In all cases, the escrow arrangement needs to be scrutinized by the SaaS customer. The MLR extracted a set of topics for vetting a SaaS-escrow arrangement in Table 4.2.

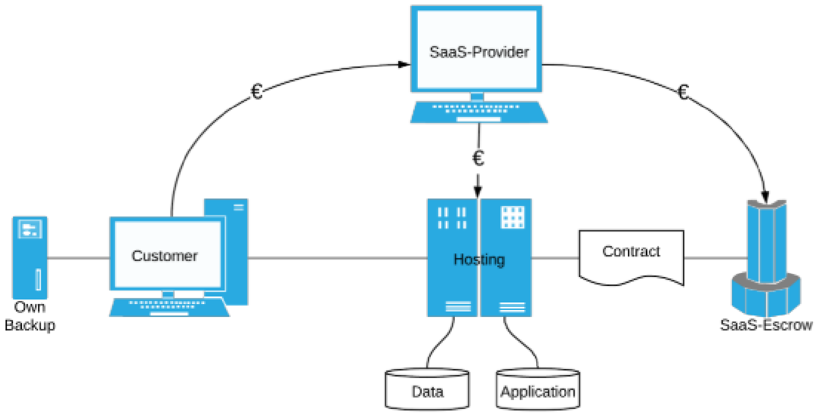


FIGURE 4.6: SaaS-escrow situation, extracted from Van Velzen, De Jong, and Jansen (2019, p. 15)

TABLE 4.2: SaaS-escrow topics for vetting contracts

Topic	Description	Source
Source code deposit	This is a listing of commands to be compiled or assembled into an executable computer program. This should include the internal repositories and third-party dependencies.	EscrowTech (n.d.), Freeman (2004), and Stulman (2008)
Data deposit	Deposit of SaaS customer data.	EscrowTech (n.d.), Freeman (2004), and Stulman (2008)
Documentation	This a board category that covers any documentation that is needed to make the new SaaS solution operational and when this needs to occur. Eg. User manuals, instructions for executing source code, and server and application configuration instructions.	EscrowTech (n.d.), Sagastume (2017), Freeman (2004), and Stulman (2008)
Frequency of deposits	The schedule of deposits containing all relevant material into the escrow vault.	EscrowTech (n.d.) and Stulman (2008)
Deposit method	The online or offline method of depositing or updating the escrow vault.	EscrowTech (n.d.), Sagastume (2017), and Stulman (2008)
Data backup and storage planning	The details about when data-backup occur and where they will be stored before the deposits are made.	EscrowTech (n.d.), Sagastume (2017), and Stulman (2008)
Technical verification	The auditing should be done on the deposit process to ensure it has been successfully completed, and the material has maintained its integrity after the deposit. This verification should produce a report containing the file listing, deposit analysis, build and compile analysis, binary comparison, and any associated test results.	EscrowTech (n.d.), Freeman (2004), and Stulman (2008)
SaaS-escrow vendor background	A background check of the vendors' history, list of clients and CVs of the C-level executives and technical staff.	EscrowTech (n.d.), Sagastume (2017), and Freeman (2004)

4.4.2 SaaS Guarantee Fund

A SaaS guarantee fund in accounting and finance is known as a a special purpose vehicle or entity. Modifying the definition of an special purpose vehicle to suit the context on this study, it is a legal entity created by a firm or group of firms for the sole purpose to financially support the continuation of SaaS services in the event that the SaaS provider enters into financial difficulty or bankruptcy (Van Velzen, De Jong, and Jansen, 2019). This fund is a separate legal entity taking the form of either a limited partnership, limited liability company, trust, or a corporation (Carey et al., 2013). They are essentially ghost firms that have no employees, make no substantive economic decisions, have no physical location, and can not go bankrupt (Carey et al., 2013). Figure 4.7 visualizes the SaaS guarantee fund situation.

These funds come with their own advantages and disadvantages. The advantages arise from the exclusion of third-party ownership over the fund. This allows for more complete control over and the ability to customize for a specific solution.

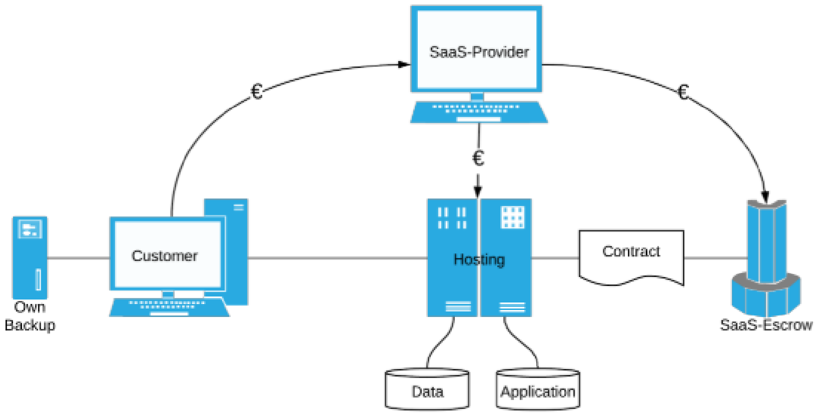


FIGURE 4.7: SaaS guarantee fund situation, extracted from Van Velzen, De Jong, and Jansen (2019, p. 15)

4.5 Service Level Agreement

SLAs are legal documents that contain quality of service requirements, usually using a number of measurable parameters that are agreed to by the SaaS provider and customer (Patel, Ranabahu, and Sheth, 2009). SLAs should be scrutinized for details about contracted support, tiers of support; how issues and inquiries are escalated, emergency response times, availability, scalability, reliability, performance, throughput, and back-up frequency (Sagastume, 2017; Alhamad, Dillon, and Chang, 2010; Gao, Bai, and Tsai, 2011). Non-performance to the agreements should also be covered by indemnity (legal and financial) clauses, and if possible, compensation clauses to breaches in agreements (Boruvka, 2016). It is common that cloud service providers (CSP) do not offer compensation as Chana and Singh (2014) state that 85% CSPs do not enforce penalties for SLA violation. A set of high-level topics identified in the MLR as critical to SaaS continuity guarantees that may be found in SLA are seen in Table 4.3.

TABLE 4.3: SLA topics for scrutinization

Topic	Description	Source
Customer support	The Cloud Service Measurement Initiative Consortium (CSMIC) (2014, p. 4), defines it as, "the response time and extent to which the CSP includes or makes available assistance to the client in their efforts to use the service, including answering questions about the service and working around or correcting any problems that may arise".	Alhamad, Dillon, and Chang (2010)
Disruption severity tiers	A disruption can have different levels of impact on business processes. CompTIA (2019) provides the following tier levels descriptions: Tier 1 systems are the highest priority and include those ICT assets that would put the business at risk with even the briefest outage. Tier 2 system outages are ones business can tolerate. They can last a few hours or up to several days before the organization is impacted. Tier 3 systems can be down for longer periods and are generally noticeable only to ICT.	Sagastume (2017)
Documentation	This is a board category which covers any documentation that is needed to make the new SaaS solution operational and when this needs to occur. This should include the build instructions which contain the steps taken when building the source code into an executable. The configuration instruction includes the steps needed for the server to run the application and any configurations.	Sagastume (2017)

Continued on next page

Table 4.3 - continued

Topic	Description	Source
Local and international policies	The policy standards that the provider follows.	Alhamad, Dillon, and Chang (2010)
Availability	A measure of being accessible and usable upon demand by an authorized entity (IT Governance Publishing, 2017).	Alhamad, Dillon, and Chang (2010) and Gao, Bai, and Tsai (2011)
Scalability	The ability of a system to allocate resources based on demand.	Alhamad, Dillon, and Chang (2010)
Reliability	A measure of the successful responses to job requests based on system specifications over a period of time (Dudouet, Edmonds, and Erne, 2015).	Alhamad, Dillon, and Chang (2010) and Gao, Bai, and Tsai (2011)
Response time	The time between the creation of a request to initiate some process and its completion.	Sagastume (2017) and Alhamad, Dillon, and Chang (2010)
Throughput	The amount of data that can be retrieved from the system in specific unit of time.	
Security	This pertains to cryptography, authentication, and authorization that affect the confidentiality, integrity and availability of data and services (Ackermann, 2012; Yu, Ren, and Lou, 2012).	Sagastume (2017), Alhamad, Dillon, and Chang (2010), and Gao, Bai, and Tsai (2011)
Privacy	This involves the collection, processing (including deletion or modification) of personal data, the rights of data subjects, and the protection of their personal data (IT Governance Publishing, 2017).	Alhamad, Dillon, and Chang (2010)
Deposit method	The online or offline method of depositing or updating the escrow vault.	Sagastume (2017)
Back-up frequency	The frequency at which back-ups of the deposited material are taken.	Sagastume (2017)
Compensation	If an SLA is broken, how or if the SaaS customer will be reimbursed.	Sagastume (2017), Alhamad, Dillon, and Chang (2010), and Boruvka (2016)
Third-party support	Information regarding the SLAs between the SaaS provider and any third-parties that will support the SaaS provider in the event that a disaster recovery plan is activated.	Sagastume (2017)

4.6 Data and Application Moveability

This section focuses on data transfer mechanisms such as, back-up and replication. Back-ups secure data from human faults, hardware problems as well as natural catastrophes (Alshammari, Alwan, and Alshaikhli, 2016). Many providers take two or three back-ups of data in practice without contractual obligation. However, this typically does not come with a warranty on the back-ups' integrity (Hon, Millard, and Walden, 2012). The format of the data is also essential. The format must be mature enough that it is compatible with other clouds or SaaS solutions. The provider should at least provide the option to return data in a .CSV format as many systems accept it.

Data replication is the act of copying data and then moving data between a company's sites, whether those be data centers, co-location facilities, public, or private clouds. Replication is handled by the SaaS provider which copies the data and moves data between the organization's sites (eg. data centers and clouds) (Phillips, 2009). It can take place amongst the following control (refer to Figure 3.2) layers: (1) application layer, uses file based replication; (2) OS layer, uses host based replication; (3) virtualization layer, uses hypervisor based replication; (4) device-driver layer, uses appliance based replication; and (5) storage layer; uses storage based replication mechanism (Saquib et al., 2013). Replication can be done using different techniques that improve available and resource consumption (Hernandez-Ramirez, Sosa-Sosa, and Lopez-Arevalo, 2012). Mirroring is a simple technique that creates a copy and places it on a different disk every time a file is stored in a disk. Total-Replication provides the highest data availability technique as stores copies of files in all available file servers. However, it requires the highest consumption of resources.

For SaaS customers that have lost access to their SaaS solution and data, it can be difficult to transfer to a new provider, or to a private cloud (Alali and Yeh, 2012). This situation is called vendor lock-in, which is the inability or difficulty for a SaaS customer to switch over to other service providers (Salleh et al., 2018). This is a result of poor compliance with portability standards such as Open Virtualization Format, and Topology and Orchestration Services for Applications. These standards aim to allow two or more kinds of cloud infrastructures to effortlessly use data and services across cloud systems (CloudWatch2, 2017).

4.7 Data Security

Cloud computing emerged from the combination of existing technologies, including service oriented architecture, virtualization, and utility computing. As a result, most data security and privacy issues are old problems in a new context (Jansen and Grance, 2011). Data security issues become more complicated due to the characteristics of the cloud ecosystem described in Section 3.1. As displayed in Figure 3.2, the SaaS provider has control over the full stack of cloud technology. This creates a dependency of the SaaS customer on the SaaS provider for implementing the appropriate data security measures (Kumar, Raj, and Jelciana, 2018). These measures must ensure that data objects in cloud servers (eg. user database and file systems), and data in transit between the cloud and the SaaS customer, including mobile data, are secured (Yu, Ren, and Lou, 2012). Data objects also include sensitive user identification information created by the user management model, service audit data, service instance information, temporary runtime data, and other data types of different values.

A SaaS provider should have a suite of security services in place to cover the full stack of security threats. ORACLE and KPMG (2020) surveyed 750 organizations and discovered that 92% of them admitted that they have a gap between current and planned cloud usage, and the maturity of their cloud security controls. Ideally, security controls should comply with industry standards, such as those see in Appendix C.1. Bibi, Katsaros, and Bozanis (2012) conducted a strengths, weaknesses, opportunities, and threats analysis of cloud computing and ranked security services pertaining to confidentiality, integrity and availability as the top security threats. From the readings of Ackermann (2012) and Yu, Ren, and Lou (2012), Table 4.4 has been constructed containing further explanations into these security service areas.

TABLE 4.4: Cloud computing security service areas

Security Area	Description	Source
Data confidentiality assurance	This protects data from being disclosed to illegitimate parties resulting in only a small group of individuals knowing the relevant security elements implemented. Encryption techniques should be used to ensure that store or transmitted data can not be read by unauthorized entities. For stored data this assurance comes through access control or rights settings in the SaaS solution. Encrypted channels such as secure sockets layer connections or virtual private networks can be used to secure transmitted data.	Ackermann (2012)
Data integrity protection	This protects data from unauthorized change to the information in transmission, storage, or processing. This includes the completeness and correctness of data as well as the correct functionality of the system. Data integrity also impacts the validity of audits on the system. If data integrity is compromised, then audit reports will yield incorrect results. To maintain data integrity, secure cryptographic hash functions, such as secure hash algorithm-2, are used to detect unauthorized changes.	Ackermann (2012)
Service auditability	Coverage of this service provides SaaS customers with monitoring capabilities in order to assess how their data is accessed and to enforce compliance with standards or SLAs. This requires the SaaS provider to invest in mechanisms to ensure an acceptable degree of transparency is achieved in regards to accessibility of data.	Yu, Ren, and Lou (2012)
Data availability	This pertains to the ability of users to access the service and data when they desire. Elements of this topic have been covered throughout this chapter and will not be discussed here. Some approaches to improving data availability involve implementation of load-balancing mechanisms, and packet filtering to protect the systems against denial of service attacks.	Ackermann (2012)

From the definitions in Table 4.4 it can be extrapolated that, to some degree, the concepts are interdependent. Data confidentiality, integrity, and service auditability are complex ,and together can form the focus of a separate study. The significance of these areas has been interpreted through the comparison of top cloud adoption risks seen in Table 3.1. However, the study's scope is primarily focused on addressing the area of availability, by concentrating on continuity guarantees and closely related concepts. Additionally, the time estimated to develop and evaluate detailed security control questions for confidentiality, integrity, and auditability will exceed this study's time frame. To compensate for these constraints, Table 4.5 provides high-level security control concepts adopted from the *Cloud Controls Matrix v3.0.1* that address confidentiality, integrity and auditability. To ease the time needed to evaluate the associated questions by experts, each control is addressed by one question in the SaaS continuity control framework. Further development of the framework will require a more granulated coverage of these controls.

TABLE 4.5: Cloud computing service security controls

Security Area	Description	Source
Application and interface security	Prior to granting customers access to data, assets, and information systems through application program interfaces, security, contractual, and regulatory requirements for customer access must be addressed. This includes the design, processes, and systems that keep a cloud application program interfaces responding to requests, securely processing data, and functioning as intended (Expedited SSL Inc, 2020).	Cloud Security Alliance (2017b)
Audit assurance and compliance	Compliance validates awareness of and adherence to corporate obligations. Audits are vital for proving or disproving compliance.	Cloud Security Alliance (2017b)
Change control and configuration	Policies and processes in use by the CSPs should ensure that only the personnel granted appropriate privileges could make use of or modify data/work products (The Cloud Service Measurement Initiative Consortium (CSMIC), 2014). Misconfigurations in internal and external security controls expose the system to unauthorized traffic can allow the spread of malicious attacks on the system (ORACLE and KPMG, 2020).	Cloud Security Alliance (2017b)

Continued on next page

Table 4.5 - continued

Security Area	Description	Source
Data security and information life-cycle	Critical vulnerabilities are addressed prior to deployment, including the analysis of source-code to detect security bugs vulnerabilities prior to the release of cloud products.	Cloud Security Alliance (2017b)
Encryption and key management	An encryption system is made up of the data, encryption engine, and key management. The encryption engine performs the mathematical process needed for encryption. Whereas the key manager handles the keys that are applied using the engine to encrypted text, or to decrypt data. SaaS providers typically only encrypt data transmissions using secure socket layer, and do not provide much encryption for the data that is stored in the cloud (Rzepka, 2012).	Cloud Security Alliance (2017b)
Identity and access management	This is focused around defining and managing the roles and access privileges of users and the reasons for the granting or denying privileges (Martin and Waters, 2018).	Cloud Security Alliance (2017b)
Threat and vulnerability management	Mechanisms in place to ensure that services are protected against known recurring cyberthreats as well as new evolving vulnerabilities (The Cloud Service Measurement Initiative Consortium (CSMIC), 2014).	Cloud Security Alliance (2017b)
Mobile device security	Mobile devices, including smartphones, laptops, and other Internet access enabled devices can expose organizational data if not properly protected (Halpert, 2004). With the emergence of the Internet of Things, any device that interacts with a cloud service supporting a SaaS presents an opportunity for malicious attacks to occur.	Cloud Security Alliance (2017b)

4.8 Data Privacy

As of May 25th 2018, the General Data Protection Regulation (GDPR) has been initiated. GDPR obliges relevant parties to provide assurance about the responsibilities and agreements between the parties (Zeker-Online, 2019). Citizens should now have more control over their personal data and actions that can be taken if personal data is misused. While data controllers and processors are now required to protect sensitive personal data by design (IT Governance Publishing, 2017). As the GDPR covers the area of data privacy, this section can be seen as an extension of what is already mentioned in Section 3.7. The GDPR is a unified law implemented by the European Union (EU) Commission, of which one of its key goals is to protect the rights, privacy, and freedoms of natural persons in the EU. IT Governance Publishing (2017) provides guidelines for compliance with GDPR standard and indicates that each organization should implement a privacy compliance framework. The framework must cover all activities that involve the collection, processing (including deletion or modification) of personal data, the rights of data subjects, and the protection of their personal data. IT Governance Publishing (2017, p. 26) states that “a privacy compliance framework is useful primarily because it provides a structured way of managing confidential data in such a way that the organization is able to comply with often complex laws and, perhaps, on a multi-jurisdictional basis.” For organizations that do not have a framework, IT Governance Publishing (2017) recommends adhering to ISO/IEC 27001:2013 and BS 10012:2017 standard in order to become GDPR compliant. Whichever approach to developing a privacy compliance framework and organization takes, it must be capable of achieving the following objectives:

- Capable of responding to subject access requests within one month.
- Capable of identifying and reporting data breaches to supervisory authorities within 72 hours.
- Capable of retaining personal data for extended periods of time.
- Capable of training staff awareness on privacy regulations.

Many of the concerns regarding data privacy are also addressed through the proper application of the security services in Table 4.4 and through privacy level agreements (CloudWatch2, 2017). A privacy level agreement is an extra attachment to the cloud service agreement contract and describes the level of privacy protection.

4.9 Testing

Business continuity and security incident response plans need to be subjected to testing at planned intervals or when significant changes occur in the organization (Zeker-Online, 2019). Incident response plans should involve impacted business entities and other business relationships that represent critical SaaS supply chain dependencies (Cloud Security Alliance, 2017a). Besides testing the response plans, testing of the SaaS environment is essential. This is done through cloud-based software testing, which is the testing and measurement activities on a cloud environment and its supporting infrastructure (Gao, Bai, and Tsai, 2011). Minor faults in one part of the system can cause cascading problems in quality of service, potentially leading to a service disruption event. For this reason, SaaS testing must validate underlying functional and non-functional components as well as the system's interoperability. Table 4.6 presents a non-exhaustive set of SaaS testing tasks and their objectives.

TABLE 4.6: SaaS testing tasks, objectives and focuses, extracted from Gao et al. (2013)

Testing Task	Objective and Focus
Component testing	Perform black-box and white-box testing for components.
Function testing	Test tenant-based service functions, behaviors, workflows, and transactions.
Integration testing	Perform integration between SaaS system and content providers, and check multi-tenant based service integration.
Deployment and recovery	Test SaaS deployment and its fault-recovery.
Multi-tenancy testing	Test multi-tenant based functions and services.
Quality of service	Assure the given quality of service requirements in SLA agreements, including scalability, reliability, availability, performance, and system through-put.
On-demand testing and simulation	On-demand large-scale test generation and simulation.
Security testing	Test single/multiple tenant-based SaaS security in databases, workflows, transactions, and functions and user privacy and system security.
Customization and configuration testing	Test the quality of tenant-based customizations and configurations in SaaS databases, workflows, user interfaces, and functional services.
Connectivity testing	Test the quality of the SaaS system's API connectivity.
User interface, portability and compatibility	Test user interfaces in usability, portability, and compatibility.
Continuous upgrade testing	Validate continuous upgrades of SaaS whenever new tenants are added, and/or existing software is changed.

4.10 Financial Stability

For this study, a simple definition of financial stability has been adopted. Financial stability is the ability of a firm to function in good times and bad, and absorb all the good and bad things that happen in the economy (Board of Governors of the US Federal Reserve System, 2018). There are many external and internal factor that affect a business. Using the financial measures presented in Turley, Robbins, and McNena (2015), Maverick (2016), and Goel (2015), attempts to provide an indication of how a SaaS provider is performing and its ability to support its business continuity plan and disaster recovery plan. Stand alone figures are not useful in determining financial stability or a business's overall health (Maverick, 2016). Therefore, measures using ratios are best suited. The ratios selected do not form an exhaustive list but is comprised of company financial health indicators. It is noteworthy to indicate that a study by Schneider et al. (2014, p.5004), on cloud certification criteria, reported that "financial stability was discouraged from being included in a certification [scheme] by four out of eight [research] participants."

4.10.1 Liquidity

It is a measure of the ability to meet short-term debt obligations without having to liquidate assets or close down. In general, the greater the coverage of liquid assets to short-term liabilities, the better as it is an indication that the organization can pay its debts while at the same time fund its ongoing operations (Turley, Robbins, and McNena, 2015).

Current Ratio measures a company's ability to pay off short-term liabilities with current assets (Kenton, 2019a). Generally, an ideal current ratio is 2:1 and typically a high ratio implies that the firm should be able to pay off its short-term debt easily (Goel, 2015). However, a very high current ratio signifies idle current assets.

$$\text{Current Ratio} = \frac{\text{Current assets}}{\text{Current liabilities}}$$

Quick Ratio focuses on the more liquid assets and leaves out inventory, which can be hard to liquidate at market value in a timely fashion (Kenton, 2019d). An ideal liquid ratio is considered as 1:1 (Goel, 2015).

$$\text{Quick Ratio} = \frac{\text{Liquid assets}}{\text{Current liabilities}}$$

4.10.2 Solvency

It is the ability to repay long-term debts and the interest on those debts. Essentially it is concerned with the long-term financial health and survival of the organization (Turley, Robbins, and McNena, 2015).

Debt Ratio measures the extent of a company's assets that are funded through long-term debt as opposed to equity. A high debt ratio signifies that the company has a lot of debt relative to its equity (Goel, 2015).

$$\text{Debt Ratio} = \frac{\text{Total debt}}{\text{Total assets}}$$

Debt-equity Ratio measures the degree to which a company has been financing its growth though loans (Hayes, 2019b). Low debt–equity ratios are favoured by investors as it indicates that their interests will be better protected if the company encounters financial hardship. The average debt–equity ratio is considered as 2:1 (Goel, 2015).

$$\text{Debt-equity Ratio} = \frac{\text{Long term liabilities}}{\text{Equity}}$$

Debt-service Coverage Ratio measures how much a company can cover its annual debt obligations using cash flow from core activities (Hayes, 2019c). A high ratio indicates a larger amount of cash flow available to satisfy annual interest and principal payments on debt (Goel, 2015).

$$\text{Debt-service Coverage Ratio} = \frac{\text{Cash flow from operating activities}}{\text{Interest expense + Installments}}$$

4.10.3 Operating Performance

The measure of difference between revenue income and expenditure for the period (surplus/deficit). A recurring operating deficit is an indication that a firm is having difficulties sustaining expenditures with its revenue income (Turley, Robbins, and McNena, 2015).

Receivables Turnover Ratio indicates how quickly short-term debt is collected or paid (Murphy, 2019b). The higher the ratio, the faster the debts are collected (Goel, 2015).

$$\text{Receivables Turnover Ratio} = \frac{\text{Net credit sales}}{\text{Average account receivable}}$$

Payables Turnover Ratio indicates how quickly a company pays off its suppliers (Murphy, 2019a). A lower ratio is desirable from a company's perspective because it shows confidence of the company's suppliers in giving credit. However, a higher ratio shows that the company pays its bills regularly (Goel, 2015).

$$\text{Payables Turnover Ratio} = \frac{\text{Net credit purchases}}{\text{Average account payable}}$$

Assets Turnover Ratio measures a company's ability to efficiently utilize its assets to generate revenue (Hayes, 2019a). A higher the ratio, the better as it indicates that the company is generating more revenue on its assets. (Goel, 2015).

$$\text{Assets Turnover Ratio} = \frac{\text{Net sales}}{\text{Total assets}}$$

4.10.4 Profitability

A measure of a company's ability to yield a profit or financial gain, representing an strong indication of its overall efficiency and performance (Maverick, 2016). A company's ability to be profitable is a strong indication of its overall health (Goel, 2015). Profitability ratio can be divided into two groups, namely, margin and return ratios. Margin ratios represent the firm's ability to translate sales into profits at various stages of measurement (Goel, 2015). Return ratios represent the firm's ability to measure the overall efficiency of the firm in generating returns for its shareholders (Goel, 2015).

Operating Margin measures how much profit a company makes on a dollar of sales, after paying for variable costs of production, such as wages and raw materials, but before paying interest or tax (Kenton, 2019c). Changes in this ratio should be observed over time and to compare the company's yearly or quarterly figures to those of its competitors. If the operating margin is increasing, its earning per dollar of sale is increasing. (Goel, 2015).

$$\text{Operating Margin} = \frac{\text{Earnings before interest and tax}}{\text{Sales}}$$

Net Profit Margin measures how much of each dollar in revenue collected by a company translates into profit (Murphy, 2020). A low profit margin is an indication of high risk as a decline in sales can possibly nullify profits and result in a loss (Goel, 2015).

$$\text{Net Profit Margin} = \frac{\text{Net income}}{\text{Sales}} * 100$$

Cash Flow Margin measures how efficiently a company converts sales into cash and provides an quality indicator of the company's earnings because it only includes transactions that involve the actual transfer of money (Kenton, 2019b). This is especially useful for comparing performance between competitors in the same industry. A negative cash flow margin is not always a bad indicator as it can be caused by investments that will result in future improvements (Goel, 2015).

$$\text{Cash Flow Margin} = \frac{\text{Cash flow from operating activities}}{\text{Sales}}$$

Return on Capital Employed measures a company's profitability and the efficiency with which its capital is used, indicating how well a company generates profits from its capital (Kenton, 2019e). This is useful for comparing the performance of companies that are involved in capital intensive activities, such as the development of SaaS products and infrastructure (Ojala, 2012; Kenton, 2019e).

$$\text{Return on Capital Employed} = \frac{\text{Earnings before interest and tax}}{\text{Total assets - Current liabilities}}$$

4.10.5 Outsourcing

The complexity of financial analysis leads may prove challenging for the intended user of this framework. ICT auditors or consultant may not have the experience needed to interpret the financial measures of the SaaS provider. Additionally, acquiring this information will require inter-department coordination as ICT personnel may not have the security clearance to access this proprietary information. Experienced financial analytic companies such as *Moody's Analytics* and *Standard and Poor's*, may need to be hired in order to properly analyze and score *Financial Stability* using their established frameworks.

4.11 European Law

Cybersecurity is a key challenge for Europe to overcome as global digitization continues (Bendiek and Schallbruch, 2019). However, cybersecurity is a dynamic area as new technologies are developed, and new threats emerge, both directing the evolution of cybersecurity policies. Addressing cybersecurity legislation is a complex issue requiring the involvement of a range of stakeholders, including legislators (Bannelier-Christakis and Christakis, 2017). For cybersecurity policies to be effective, multiple policy areas need to be combined to elicit horizontal requirements, while creating measures addressing vertical requirements at the EU and Member State levels (Wessel, 2015). It is commonly agreed that the legislator is in particular responsible for setting up an appropriate regulatory framework within which private and public entities could carry out their tasks and duties. This is driven by the implementation of directives and regulations. To understand the degrees of influence between a directive and a regulation, the explanations from Rotondo (2013) are used:

- *Directives:* Provide a set of results that must be achieved by each Member State, allowing national authorities to choose their own methods to transpose directives into national laws.
- *Regulations:* Have binding legal force throughout every Member State without the need for transposition into national law by each Member State. Regulations are directly applicable to the Member States of the EU.

At the time of writing, Directive (EU) 2016/ 1148 and Regulation (EU) 2019/ 881 are found to be prominent legislation and focused on the development of cybersecurity in the EU. Schulz and Korčok (2016, article 1) (Directive (EU) 2016/ 1148) states that "this directive lays down measures with a view to achieving a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market." This Directive views information system security as the resilience of a system to resist or recover from actions that compromise the availability, authenticity, integrity or confidentiality of consumed or offered data and services (Fuster and Jasmontaite, 2020). Following this, Tajani and Ciamba (2019, article 1) (Regulation (EU) 2019/ 881) states its aim as "ensuring the proper functioning of the internal market while aiming to achieve a high-level of cybersecurity". To do so it lays out objectives, tasks and organisational matters relating to the *European Union Agency for Cybersecurity* (ENISA), and a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity.

4.11.1 Dutch Law

As this study is geared towards the Dutch industry, applicable laws must be acknowledged. The Dutch Law system is outside the researcher's experience, understanding, and linguistic ability. Therefore, only applicable laws that are clearly stated in literature have been are mentioned. The Zeker-Online (2019) framework of standards is aimed at achieving similar goals to this study. In the framework, they list the three legal controls applicable to Dutch SaaS providers outside of GDPR laws seen below:

- The service provider declares Netherlands law applicable to the service and to any disputes about the service that may arise with entrepreneurs.
- The service provider complies with the statutory obligations, including the information obligations prescribed by articles 3:15d, 6:227b and 6:227c of the Civil Code.
- The service provider supplies the service in a manner that ensures that entrepreneurs can comply with the provisions of articles 47 to 53 inclusive of the State Taxes Act (Algemene Wet Rijksbelastingen).

4.12 Takeaways

Following the design science research (DSR) approach described in Chapter 2, a set of concepts has been synthesized and discussed throughout this chapter. As expected, some of these concepts were not evident during the construction of the certification framework concept of the conceptual-model in Figure 1.1 and 3.5. Thus, it is necessary to revise the conceptual-model to show the progress of this study at this point in time. Figure 4.8 shows version 3 of the conceptual-model. The contributing findings are listed:

- The naming of some certification framework concept's attributes has changed to reflect correct industry terminology. The *technology maturity* attribute has been removed as this is associated with maturity models, which this study's framework is not intended to be.

- The sections of this chapter identify sub-concepts that become requirements for the framework and formulate the framework's questions. Where applicable, these sub-concepts are highlighted using tables and lists.

- The following attributes have been added to the conceptual-model: *service level agreement*, *data and application migration*, *testing*, and *data privacy*.

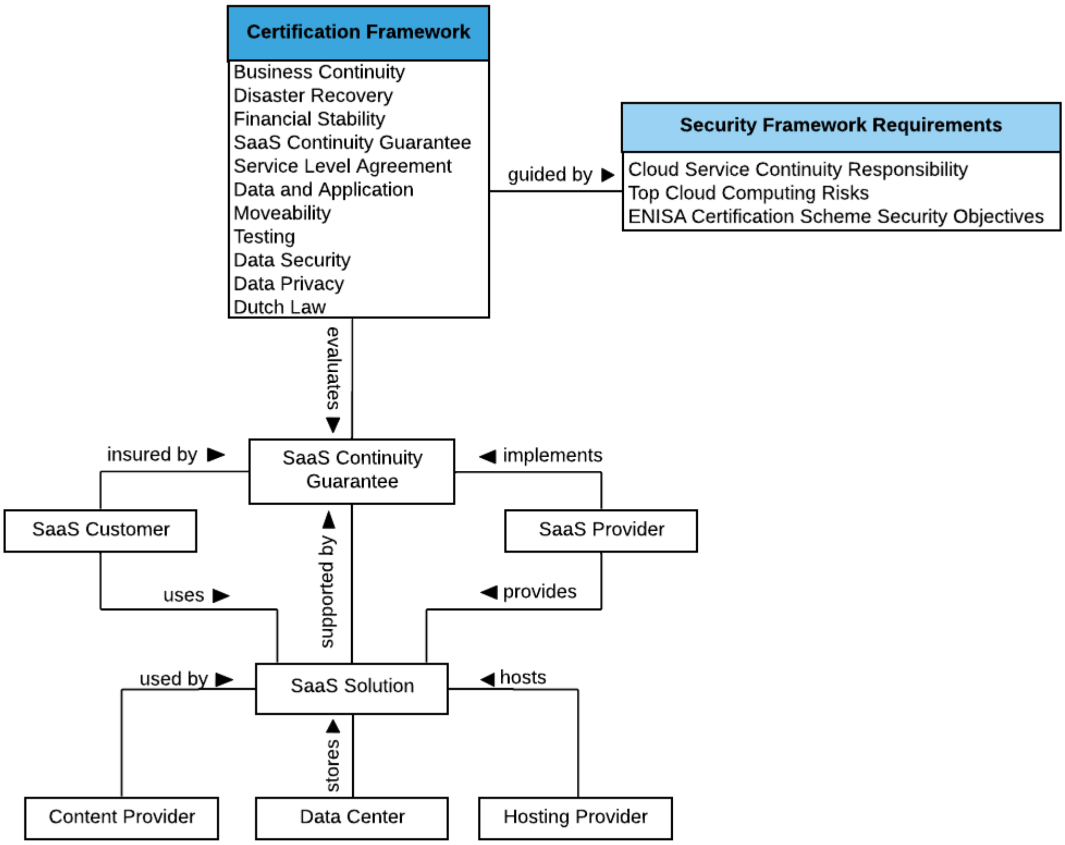


FIGURE 4.8: Research context conceptual-model version 3

Chapter 5

Framework Draft Design

5.1 Introduction

This chapter traces the decisions made during the construction phase of the software as a service (SaaS) continuity control framework draft, described in Section 2.3.5. Features of the framework are also traced to previous sections and figures. This is done to provide clarity into the sources of influence that have lead to decisions impacting the design of the framework's first draft. In Chapters 3 and 4, literature relevant to the cloud ecosystem in Europe, and risks affecting SaaS were examined in order to elicit framework requirements grounded in existing literature. Following the design science research (DSR) life cycle displayed in Figure 2.1, the study has iterated through the *rigor*, *relevance* and *design cycles*. These cycles are in continuous iteration to account for newly acquired knowledge and challenges, until a satisfactory framework is created (Shrestha, Cater-steel, and Toleman, 2014).

Important to note, the topics of *European law* discussed in Section 4.11, *back-up strategy* discussed in Section 4.3.1, and *cloud computing service security controls* displayed in Table 4.5 are not included in the framework draft discussed in this chapter. These topics as well as some minor topics have been added to Chapter 4.1 during the expert evaluation phase, which occurs after the creation of the first draft of the framework.

5.2 Requirements and Grounding

The *Rigor* and *Relevance Cycles*, have identified European Union requirements for cloud service provider (CSP) certification schemes and SaaS relevant concepts grounded in scientific and grey literature sources. In section 3.7, the cloud technology stack and a SaaS providers range of control were discussed (Figure 3.2) along side the legal implications of General Data Protection Regulation (GDPR) on data controllers and data processors. Following this, section 3.8 compares the top five cloud computing risks of literature in Table 3.1 to assist in modifying the cloud computing risk ontology adopted from Dutta, Peng, and Choudhary (2013). In doing so the highest layer of the framework, the risk domain layer, was identified by using the sub-categories of the risk ontology (Figure 3.3) listed below.

- Business Continuity
- Disaster Recovery
- Continuity Guarantee
- Service Level Agreements
- Data and Application Migration
- Financial Stability
- Testing
- Data Security

- Data Privacy
- Dutch Law

In Section 3.9, the definition of a security framework provides requirements for an framework that is suitable for certificating CSPs, adding clarification to the required path of the study. Additionally, the design of the *Cloud Controls Matrix v3.0.1* has been identified as a suitable candidate for a benchmark design to follow (Cloud Secuirty Alliance, 2014). In Section 3.10, the *Cloud Service Provider Certification* scheme provides design recommendations/ requirements for achieving security objectives, as well as a guide for frameworks in achieving recognition by *European Union Agency for Cybersecurity* (ENISA) as a basic, substantial, or high risk assurance level certification (Barreira et al., 2019). Throughout the sections in Chapter 4, the risk domains have been investigated, and risk mitigation controls identified. These controls became a sub-layer of the framework. For each control, topics for vetting information about controls are identified, and questions formulated.

5.3 Framework Draft

From the *Design Cycle*, drafts of the framework's procedures and design are created in preparation for evaluation through expert interviews and case studies. As discovered during the MLR, existing security frameworks for assessing CSPs differ in the degree of focus place on specific domains. Focus is typically placed on either the technical or the business side (Moravcik, Segec, and Kontsek, 2018). This study's framework attempts to find a balance between the business and technology facets, as business continuity places emphasis on supportive business processes, while SaaS is technology oriented. The framework's structure follows that of the *Cloud Controls Matrix v3.0.1* mentioned in Section 3.9. The framework exists as an *MS Excel* file containing number of sheets supporting its use.

To provide a more detailed understanding of the structure of the framework a UML class diagram has been constructed and visualized in Figure 5.2. A UML class diagram can be used to describe a static view the framework, and is composed of classes, attributes and the relationships between classes (Purchase et al., 2003). Guidelines for creating the UML diagram were followed from Ambler (2005). Some of the feature requirements for the draft were identified by comparing existing frameworks, see Section 5.5. The first iteration of the construction phase has materialized the high-level features seen below:

- *User Guide:* Provides a guide in how to use the features of the framework and explains the purpose of the other sheets in the file. It also contains the copyright for the framework, as well as authorship information. See Appendix C.2.
- *Questionnaire:* Contains the questions and answer inputs as well as descriptions about the controls being addressed by the questions. For tractability purposes, the literature sources that inspired the controls and questions are stated, along with the location of the information in the study's paper. See Figure 5.3
- *Questionnaire Report:* Contains the the report of the answers entered into the questionnaire matrix and the resulting certification mark. It summarizes the count of answer input types (satisfactory, partially satisfactory, not satisfactory, and not applicable) associated with each domain, allowing for a review of the weak and strong domains of the SaaS provider. Additionally, it indicates if

any question has not been answered. It is part of the process to verify as the calculations involved with the determination of the certification mark depend on the answering of all questions. See Appendix C.3.

- *Standards:* Contains a a table of standards that can be used as a reference in the event that a SaaS provider has other certifications that may provide evidence to answer the framework's questions. See Appendix C.1.
- *Change Log:* Assists in trace the changes made to questions by allowing the user to record the change made, date and influence/ reason of the change. See Appendix C.4.

The more granulated levels of the initial draft consists of 10 risk domains, with a total of 25 controls identified, and 127 questions used to assess the controls. When compared to the questions count of the *Cloud Controls Matrix v3.0.1* and *Zeker-Online* frameworks, which contain approximately 300 questions each (Zeker-Online, 2016), it can be extrapolated that the development of this framework is on the correct path. Due to the size of the questionnaire matrix, a snippet is displayed in Figure 5.3 with dummy data inputs.

5.4 Answer Input Levels

Within the *Questionnaire*, the answer inputs available to the user are: *satisfactory*, *partially satisfactory*, *not satisfactory*, and *not applicable*. The decision to use these answers arises from the complication of addressing the 10 differing domains of the framework. This multi-layered answer feature can be seen in maturity model designs, and is an expected result from framework construction guidelines explained in Section 2.3.5. As such, assistance for providing guidance in the interpretation of the answer input levels is found in the maturity levels defined by Najjar and Al-Sarayreh (2015). Najjar and Al-Sarayreh (2015) lists five maturity levels which help organizations apply improvements to a set of related processes:

- *Initial:* There is no formal process.
- *Defined:* Processes are well characterized and understood, and are described in standards, procedures, tools, and methods.
- *Managed:* There is a minimal process and the status of projects is visible to management at major milestones.
- *Quantitatively managed:* The organization and projects establish quantitative objectives for quality and process performance and use them as criteria in managing processes.
- *Optimizing:* All processes are already defined and managed. Goals for levels one to four are all achieve.

The application of the five levels is not suitable for a number of the framework's questions. This is a result of the variety of domains the questions address and the differing granularity levels of the questions. To compensate, broadly interpreted definitions have been created by combining the five levels defined by Najjar and Al-Sarayreh (2015). *Optimizing* and *quantitatively managed* are merged to form *satisfactory*, *managed* and *defined* merge to form *partially satisfactory*, and *initial* is equivalent to *not satisfactory*. As such, these mergers form the guidelines for what qualifies as *satisfactory*, *partially satisfactory*, *not satisfactory*, and *not applicable* seen below:

- *Not applicable:* The question addresses a concept that is not relevant to the SaaS provider's context.
- *Not satisfactory:* The evidence produced by the SaaS provider for the concept addressed by the question, can be interpreted by the user of framework in such a way that the concept is not formally characterized and understood, with no supporting processes implemented. For *yes* or *no* questions this is equivalent to *no*.
- *Partially satisfactory:* The evidence produced by the SaaS provider for the concept addressed by the question, can be interpreted by the user of framework in such a way that the concept is formally characterized and understood, with minimal supporting processes implemented.
- *Satisfactory:* The evidence produced by the SaaS provider for the concept addressed by the question, can be interpreted by the user of framework in such a way that the concept is defined and managed using quantitative objectives for determining quality and performance. For *yes* or *no* questions this is equivalent to *yes*.

5.5 Security Framework Comparisons

By comparing the SaaS continuity control framework against existing frameworks, gaps and similarities can be identified. The frameworks are selected based on the following acceptance criteria: (1) must be freely accessible; (2) covers a wide range of cloud specific security control domains; and (3) fits the definition for a security framework seen in Section 3.9. A non-exhaustive list consisting of two frameworks have been identified, namely, *Cloud Controls Matrix v3.0.1*, from *Cloud Security Alliance*, and *Zeker-Online Framework (ZOF)* from *Zeker-Online*. Notably, the *Cloud Controls Matrix v3.0.1* artefact acts as a support/ traceability tool for the *Consensus Assessment Initiative Questionnaire v3.1* artefact acts as the auditing questionnaire. These two artefacts are two sides of the same coin. For this reason they are seen as one artefact, namely *(CCM)*, when comparing frameworks.

5.5.1 Layout Feature Comparison

Existing frameworks can be expected to contain layout features that benefits the CSP certifying process. By examining features, the researcher can identify requirements that improve the framework's **operational feasibility** and **ease of use** criteria as described in Table 2.4. In Table 5.1, the features which are present in a framework are marked by a check-mark, excluding the *document type* feature which is either a spreadsheet (*S*); example, *MS Excel*, or a text document (*T*); example, *MS Word*. The only features that are missing in the SaaS continuity control framework are the cloud technology layer mapping and cloud service deployment layer mapping. These have been intentionally left out as the value added regarding the aim of the study is small in comparison to the workload required to accurately implement the features.

TABLE 5.1: Identification of the presence of layout features in SaaS continuity control framework (SCF), CCM, and ZOF to ensure that no significant features are missing in the SCF

Layout Feature	SCF	CCM	ZOF
Authorship/ acknowledgement	✓	✓	✓
Change Log	✓	✓	
Control ID	✓	✓	✓
Control name	✓	✓	✓
Control description	✓	✓	✓
Copyright	✓	✓	✓
Cloud technology layer mapping (See Figure 3.2)		✓	
Cloud service deployment layer mapping (See Figure 3.1)		✓	
Document type	S	S	T
Domain ID	✓	✓	✓
Domain name	✓	✓	✓
Introduction/ instructions	✓	✓	✓
Question	✓	✓	✓
Question answer options	✓	✓	
Question ID	✓	✓	
Question notes	✓	✓	
Standards	✓	✓	
Terms of use	✓	✓	✓

5.5.2 Domain & Topic Comparison

The frameworks differ in their use of terminology, domains, and assignment of topics to domains. To combat this inconsistency, the high-level domains of the three frameworks were compared in Table 5.2. As a topic may exist in one or more domains across the frameworks, words from the domains' titles were used in word searches across the three frameworks. Allowing for the identification of the topic locations across domains. Topics have different levels of coverage depth across the frameworks. Due to this, an assignment of coverage level is needed.

Table 5.2 provides an indication of not only the gaps in the SaaS continuity control framework, but also gaps in the other frameworks that the SaaS continuity control framework fills. This can be seen in the lack or shallow coverage of the other frameworks in *continuity guarantee*, *cloud testing*, *disaster recovery*. *Financial stability* is not considered to have *D* level coverage as this study addresses with only three questions despite the number of ratios mentioned in Section 4.10. The inclusion of only three questions is a result of the study's inability to identify quantifiable benchmarks for the ratios. Only two ratios have benchmarks that enable their use in the framework. The gaps in the SaaS continuity control framework condense around domains that oriented are technical data security controls. To compensate for this, the concept of method enrichment from method engineering is adapted for use in this situation,

5.5.3 Framework Enrichment

Entities can enrich their artefacts by adopting concepts from the publicly available sources (Weerd and Brinkkemper, 2008). The framework comparison, revealed a number of gaps in the SaaS continuity control framework. Due to limited manpower and time in this study, these gaps were filled by enriching the framework with existing controls and questions from the *Cloud Controls Matrix v3.0.1* and *Zekker-Online Framework*. The controls and questions enriched from *Cloud Controls Matrix v3.0.1*

TABLE 5.2: Determination of the degree of security control coverage by identifying questions addressing each topic in the SaaS continuity control framework (SCF), CCM, and ZOF. Based on the level of coverage a topic in a framework, it is either assigned to have domain level coverage (*D*); meaning a topic is coverage extensively, or mentioned within a domain (*M*); meaning a topic is mentioned but is not covered as extensively

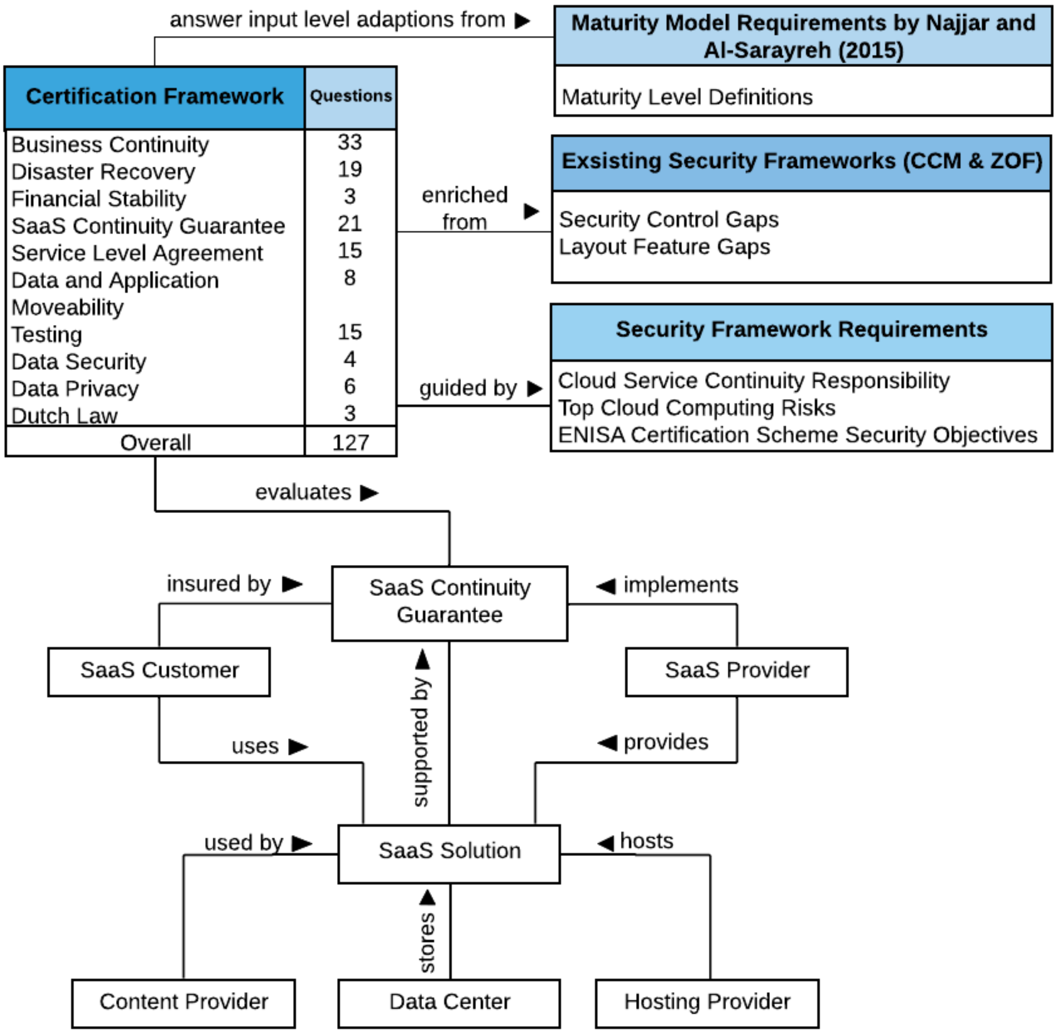
Security Control Topic	**SCF**	**CCM**	**ZOF**
Application & interface security	M	D	D
Audit assurance & compliance	M	D	D
Business continuity & operational resilience	D	D	D
Change control & configuration Management	M	D	D
Cloud testing	D	M	
Continuity guarantee	D		
Data privacy	D	M	D
Data security & information lifecycle management	M	D	D
Disaster recovery	D	M	M
Dutch law	D		D
Financial stability	M		
Governance & risk management	M	D	D
Human resources		D	
Identity & access management	M	D	M
Infrastructure & virtualization security	M	D	D
Interoperability & portability	D	D	
Service level agreements	D	M	D
Security incident management, E-discovery, & cloud forensics	M	D	M
Supply chain management, transparency, & accountability	M	D	
Terms & conditions	M	M	D
Threat & vulnerability management	M	D	D

are primarily used in the data security domain. Where as the questions used in the Dutch law domain are from *Zekker-Online Framework*.

5.6 Takeaways

Following the framework construction phases described in Section , a draft of the SaaS continuity control framework has been constructed. This process has resulted in an updated version of the research context conceptual-model discussed in Chapter 4, and the updated visualized in Figure 5.1. The draft has been populated with a number of features that have been discussed throughout this chapter:

- Answer input levels have been defined by adapting the definitions of maturity level from Najjar and Al-Sarayreh (2015).
- Gaps are identified in the SaaS continuity control framework by conducting a comparison with existing frameworks, and where applicable are compensated for.
- The first draft of the SaaS continuity control framework has been created for evaluation in expert interviews, further discussed in Chapter 6.



Certification Framework	Questions
Business Continuity	33
Disaster Recovery	19
Financial Stability	3
SaaS Continuity Guarantee	21
Service Level Agreement	15
Data and Application Moveability	8
Testing	15
Data Security	4
Data Privacy	6
Dutch Law	3
Overall	127

answer input level adaptions from ▶
Maturity Model Requirements by Najjar and Al-Sarayreh (2015)
Maturity Level Definitions
enriched from ▶
Exsisting Security Frameworks (CCM & ZOF)
Security Control Gaps
Layout Feature Gaps
guided by ▶
Security Framework Requirements
Cloud Service Continuity Responsibility
Top Cloud Computing Risks
ENISA Certification Scheme Security Objectives
evaluates ▶
insured by ▶
SaaS Continuity Guarantee
◀ implements
SaaS Customer
SaaS Provider
supported by ▶
uses ▶
◀ provides
used by ▶
SaaS Solution
◀ hosts
stores ▶
Content Provider
Data Center
Hosting Provider

FIGURE 5.1: Research context conceptual-model version 4

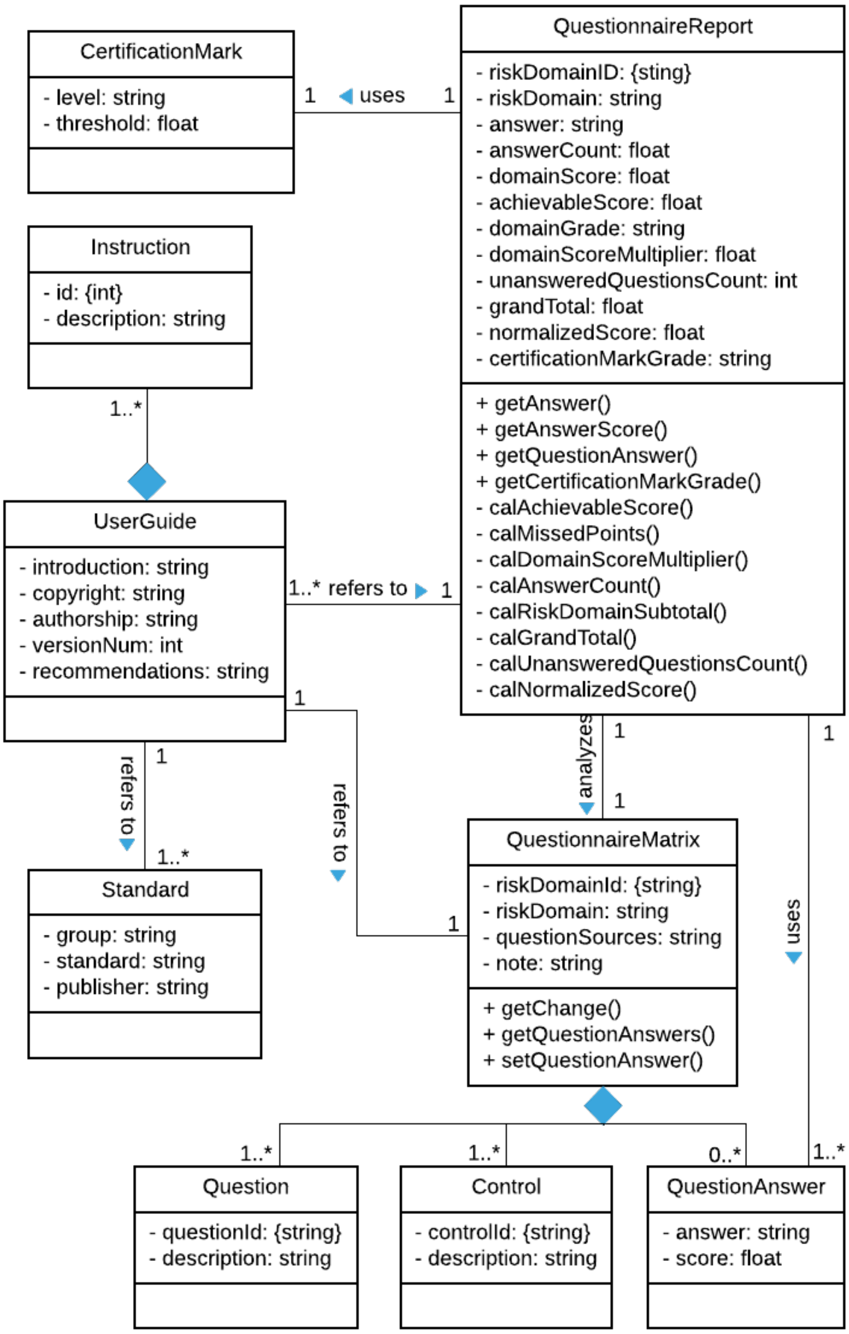
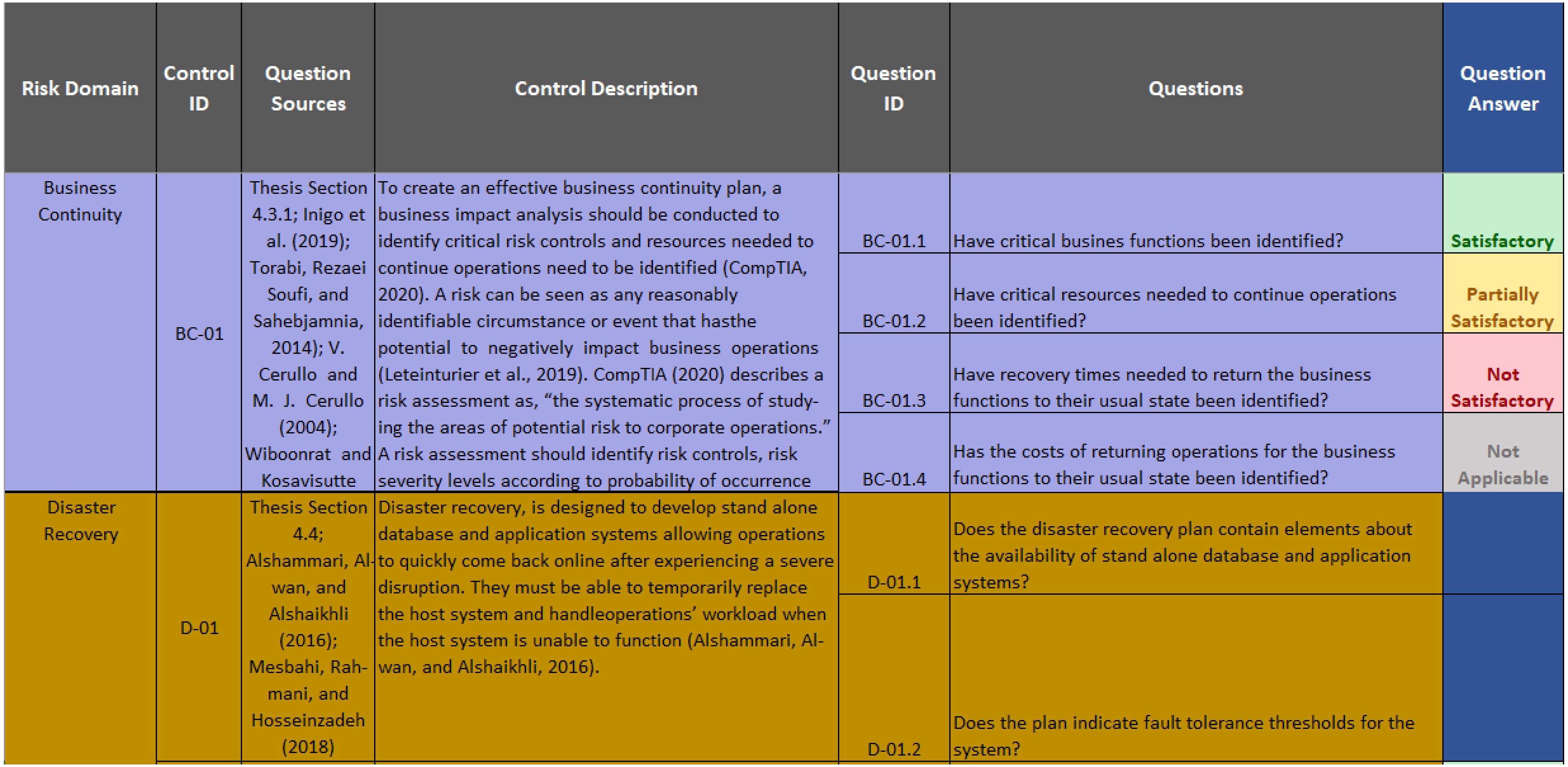


FIGURE 5.2: UML class diagram of the the SaaS continuity control framework's informational structure



Risk Domain	Control ID	Question Sources	Control Description	Question ID	Questions	Question Answer
Business Continuity	BC-01	Thesis Section 4.3.1; Inigo et al. (2019); Torabi, Rezaei Soufi, and Sahebjamnia, 2014); V. Cerullo and M. J. Cerullo (2004); Wiboonrat and Kosavisutte	To create an effective business continuity plan, a business impact analysis should be conducted to identify critical risk controls and resources needed to continue operations need to be identified (CompTIA, 2020). A risk can be seen as any reasonably identifiable circumstance or event that hasthe potential to negatively impact business operations (Leteinturier et al., 2019). CompTIA (2020) describes a risk assessment as, "the systematic process of studying the areas of potential risk to corporate operations." A risk assessment should identify risk controls, risk severity levels according to probability of occurrence	BC-01.1	Have critical busines functions been identified?	Satisfactory
				BC-01.2	Have critical resources needed to continue operations been identified?	Partially Satisfactory
				BC-01.3	Have recovery times needed to return the business functions to their usual state been identified?	Not Satisfactory
				BC-01.4	Has the costs of returning operations for the business functions to their usual state been identified?	Not Applicable
Disaster Recovery	D-01	Thesis Section 4.4; Alshammari, Al-wan, and Alshaikhli (2016); Mesbahi, Rahmani, and Hosseinzadeh (2018)	Disaster recovery, is designed to develop stand alone database and application systems allowing operations to quickly come back online after experiencing a severe disruption. They must be able to temporarily replace the host system and handleoperations' workload when the host system is unable to function (Alshammari, Alwan, and Alshaikhli, 2016).	D-01.1	Does the disaster recovery plan contain elements about the availability of stand alone database and application systems?	
				D-01.2	Does the plan indicate fault tolerance thresholds for the system?	

FIGURE 5.3: Questionnaire snippet of framework draft

Chapter 6

Expert Evaluations

6.1 Introduction

In this chapter, the results of the *ex-ante* design product are presented following the evaluation strategy described in Section 2.4. The results have been derived from semi-structured expert interviews aimed at eliciting opinions and knowledge from the experiences of the experts. Prat, Comyn-Wattiau, and Akoka (2015) encourages researchers to create new evaluation methods combining what is being evaluated and how it can be done. To attempt this, if the interviewee is willing and there is ample time, protocol analysis and brainstorming is encouraged during the framework question evaluation stage. Each interview consists of four stages, namely: (1) the background investigation; (2) framework question evaluation using 5-point Likert scales; (3) overall framework evaluation using open-ended questions; and (4) closing questions/ comments. The documents used for the expert interviews can be found in Appendix B. The resulting findings are elaborated on in this chapter.

6.2 Ex-ante Evaluation Objectives

The framework is evaluated on the criteria of **operational feasibility**, **ease of use**, **completeness**, and **usefulness**. The definitions of these criteria have been extracted from Prat, Comyn-Wattiau, and Akoka (2015) and adapted to the study's context, seen in Table 6.1. The aims of addressing these criteria are: (1) identify modifications to existing framework elements; (2) elicit new framework requirements; and (3) ensure that the development of the framework is on the correct path to achieving the aim of the study. Which is *to improve the transparency of the software as a service (SaaS) industry by designing and evaluating a certification framework that can be used to analyze SaaS continuity control risks, and award certification marks to SaaS providers, in order to foster improvements in risk awareness and customer trust in SaaS*.

TABLE 6.1: Evaluation criteria and definitions

Criteria	Adapted definition for this study	Evaluation Tool
Usefulness	To what degree does the framework extract insightful information for awarding a certification mark?	5-point Likert scale
Ease of use	What is the degree of difficulty associated with gathering the information required by framework?	5-point Likert scale
Operational feasibility	To what degree do the experts see the framework being used by individuals in practice?	Open-ended questions
Completeness	To what degree does the framework assess critical risk concepts relating to SaaS continuity controls, and contain necessary questions for adequately assessing these concepts?	Open-ended questions

6.3 Expert Search Results

Due to the COVID-19 pandemic and the world wide disruption caused by it, there is a possibility that experts in the information communication and technology (ICT) industry, especially SaaS, would be busy compensating for changes caused by the pandemic. As a result, extra focus is placed on attracting attention to the research using the LinkedIN approach documented in appendix A.3. The use of an automatic connection tool allowed 916 potentially interested individuals to be contacted. Of that number, have 30 expressed interest in contributing to the research by providing an e-mail address to receive further information. If such a response is received from an individual, a background check is done to ensure that the individual meets the criteria set in Section 2.4.1. The interview protocol is then sent to the expert, including the interview consent form, to be signed and returned providing confirmation of their participation. From the 30 who expressed interested in contributing, only eight returned signed copies of the interview protocol. As such, only eight usable interviews have been completed. Information regarding the interviews is displayed in Table 6.2.

6.4 Interviewed Experts

In this study, purposive sampling is used to select experts with experience in one or more of the framework domains discussed in Chapter 4. This type of sampling requires participants to be selected based on their qualities (Etikan, 2016). Additionally, this technique addresses the issue of the willingness of individuals to participate, and their ability to effectively communicate experiences and opinions enabling the researcher to reflect on the information (Etikan, 2016). To support this technique, the following criteria are used to highlight candidate: (1) a prospective candidate must have a minimum two years of experience in at least one of the framework's risk domain; (2) a prospective expert must speak English; and (3) able to conduct the interview online due to the COVID-19. Table 6.2 displays the characteristics of the experts as well as the domains they evaluated.

TABLE 6.2: Interviewee characteristics and evaluated domains. Domains have been coded as follows: business continuity (BCO), disaster recovery (DRE), continuity guarantee (CGU), service level agreement (SLA), data and application migration (DAM), data security (DSE), data privacy (DPR), financial stability (FSA), testing (TES), dutch law (DLA)

ID	Role	Experience	Country	BCO	DRE	CGU	SLA	DAM	DSE	DPR	FSA	TES	DLA
I-1	Entrepreneur	11 years	Netherlands									X	
I-2	Consultant	34 years	Netherlands	X	X		X	X				X	
I-3	Developer	6 years	Belgium	X			X			X			
I-4	Consultant	19 years	Australia	X	X		X		X		X		
I-5	Product Manager	10 years	U.S.A			X							
I-6	Consultant	20 years	India	X	X	X	X	X				X	
I-7	ICT Manager	3 years	U.S.A	X	X		X	X			X		
I-8	Consultant	1.8 years	Netherlands						X				

Expert Selection Criteria Exception

An exception has been made for expert *I-8* as he does not meet the minimum of two years experience in the data security domain at the time of the interview. However, by the end of the study he would have two years of of experience in data security. The decision to use the resulting feedback has been made to compensate for the lack of evaluations on the changes discussed in Section 7.5, and the lack of time remaining until the end of the evaluation phase. Upon completion of the expert's interview, only two days remained until the deadline for conducting interviews.

6.5 Quantitative Evaluation Results

The evaluation method used in the interviews collects quantitative data for determining a SaaS provider's degrees difficulty in gathering the information required to answer the questions posed by the framework, and degrees of usefulness of the insights gathered from each question. Quantitative data is collected on the framework's **ease of use** and **usefulness** criteria using a 5-point likert scale. The degree of **usefulness** is selected by the expert using the following scale (each option has assigned points): **very useless** (1 point), **useless** (2 points), **neutral** (3 points), **useful** (4 points) and **very useful** (5 points). Similarly, the degree of **ease of use** is selected using the following scale (each option has assigned points): **very difficult** (1 point), **difficult** (2 points), **neutral** (3 points), **easy** (4 points) and **very easy** (5 points). The evaluation results for each question are recorded using a modified version of the *questionnaire*, seen in Appendix B.5. The average of the points per question is calculated, and are displayed in Table 6.3, along with the number of questions added during the evaluation phase, and the resulting question count.

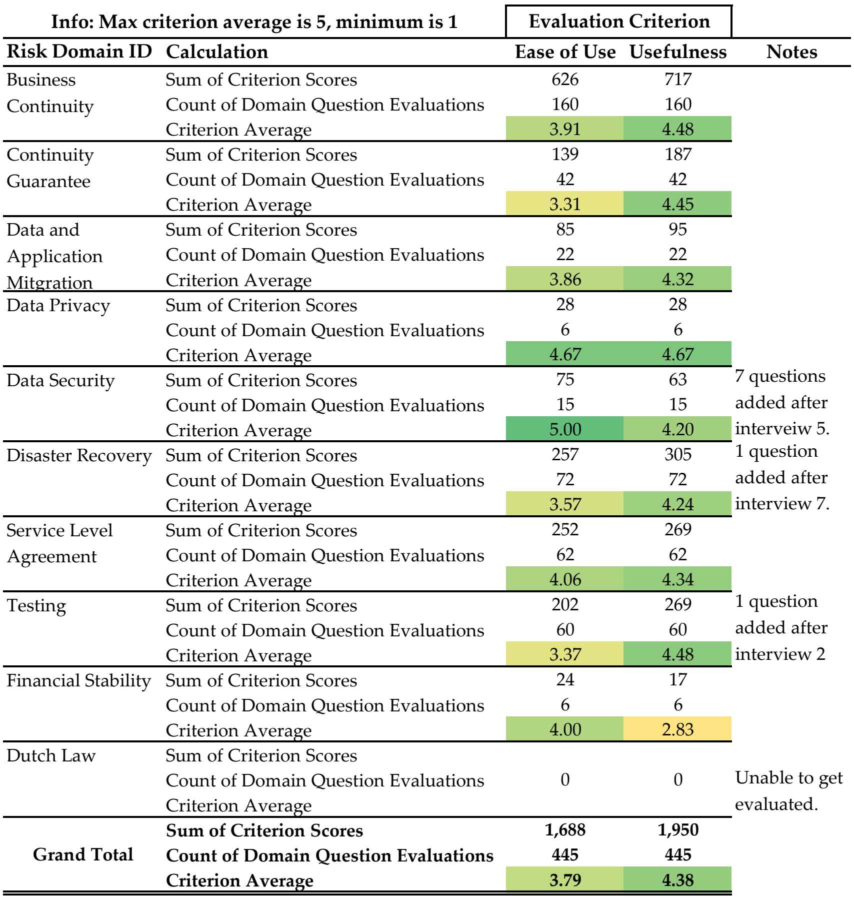
A threshold of a 3 point average is used for both criteria to flag questions as poorly performing. Every flagged question is then placed under consideration for removal from the framework. Using the knowledge gained from the study and notes taken during the evaluation phase, a decision is made whether to remove the question or not. Additions and removals made to the framework are elaborated on in Chapter 7. Furthermore, findings at the framework, domain, and question granularity levels are discussed in this section, using the evaluation average reports and histograms in Figures 6.1, 6.2, and 6.3 and question level average reports and histograms available from `https://saascontinuityframework.com/framework/`. The histograms provide transparency into the distribution of scores that have resulted in the averages seen in Table 6.3.

6.5.1 Framework Level Findings

Based on the overall average evaluation scores seen in Table 6.3, the framework's **ease of use** is between **neutral** and **easy**, whereas its **usefulness** is between **useful** and **very useful**. To provide transparency, Figure 6.1 visualizes the distribution of scores for both criterion. Based on the conversations held with the experts when explaining the study's interpretation of **ease of use**, there have been indications to suggest that there is a degree of inconsistency in their understandings of the **ease of use** criterion. This may create some degree of misrepresentation of the level of difficulty in collecting evidence to answer questions. However, this is not seen as a critical issue in the framework as it only impacts the time required to fulfill the framework's requirements. Therefore it does not impact the aim of the framework which is to identify the level of risk associated with a SaaS provider's continuity controls.

Concerning the **usefulness** criterion, no such indications of inconsistencies in the experts' understandings of the criterion have been noticed. With no known issues with the **usefulness** score of the framework, Figure 6.1 indicates that 87% of the

TABLE 6.3: Domain evaluation results before the removal of any questions, with a total question count of 136



Info: Max criterion average is 5, minimum is 1		Evaluation Criterion		
Risk Domain ID	**Calculation**	**Ease of Use**	**Usefulness**	**Notes**
Business Continuity	Sum of Criterion Scores	626	717	
	Count of Domain Question Evaluations	160	160	
	Criterion Average	3.91	4.48	
Continuity Guarantee	Sum of Criterion Scores	139	187	
	Count of Domain Question Evaluations	42	42	
	Criterion Average	3.31	4.45	
Data and Application Mitgration	Sum of Criterion Scores	85	95	
	Count of Domain Question Evaluations	22	22	
	Criterion Average	3.86	4.32	
Data Privacy	Sum of Criterion Scores	28	28	
	Count of Domain Question Evaluations	6	6	
	Criterion Average	4.67	4.67	
Data Security	Sum of Criterion Scores	75	63	7 questions added after interveiw 5.
	Count of Domain Question Evaluations	15	15	
	Criterion Average	5.00	4.20	
Disaster Recovery	Sum of Criterion Scores	257	305	1 question added after interview 7.
	Count of Domain Question Evaluations	72	72	
	Criterion Average	3.57	4.24	
Service Level Agreement	Sum of Criterion Scores	252	269	
	Count of Domain Question Evaluations	62	62	
	Criterion Average	4.06	4.34	
Testing	Sum of Criterion Scores	202	269	1 question added after interview 2
	Count of Domain Question Evaluations	60	60	
	Criterion Average	3.37	4.48	
Financial Stability	Sum of Criterion Scores	24	17	
	Count of Domain Question Evaluations	6	6	
	Criterion Average	4.00	2.83	
Dutch Law	Sum of Criterion Scores			
	Count of Domain Question Evaluations	0	0	Unable to get evaluated.
	Criterion Average			
Grand Total	**Sum of Criterion Scores**	**1,688**	**1,950**	
	Count of Domain Question Evaluations	**445**	**445**	
	Criterion Average	**3.79**	**4.38**	

$$\text{Criterion average} = \frac{\text{Sum of Criterion Scores}}{\text{Count of Domain Question Evaluations}}$$

scores are either **useful** or **very useful**. This strengthens the study's interpretation of the framework's overall **usefulness** score average. Noticeably, 19% of the **ease of use** scores and 10% of **usefulness** scores are **neutral**. It has been expected that experts would have stronger opinions on the questions and would not award a significant number of **neutral** scores. This can be associated with central tendency bias in which participants may avoid extreme response categories when scoring questions that they feel uncertain about (Emerson, 2017).

6.5.2 Domain Level Findings

As seen in Table 6.3, the average **ease of use** scores for the *disaster recovery*, *continuity guarantee*, *data and application migration* and *testing* domains are between **neutral** and **easy**. This rating does not degrade the value of the framework, in fact, it provides some insight into the time required to gather the evidence for these domains. This can be communicated to the SaaS provider ahead of time, providing insights into the workload required by the SaaS provider to prepare for the assessment of these domains. The only domain to perform poorly in the **usefulness** criterion is *financial stability*.

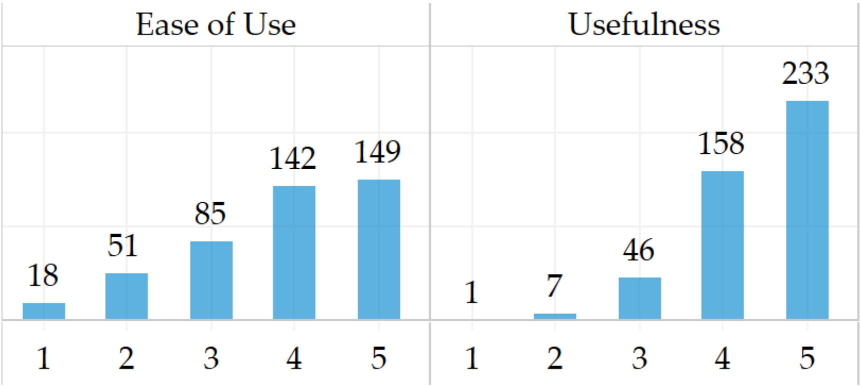


FIGURE 6.1: Framework ease of use and usefulness score distribution

It has an average **usefulness** score that is between **neutral** and **useless**, flagging it for removal. The distribution of the domain's scores, seen in Figure 6.3 does not provide a definite indication to support its removal. However, this decision is supported by Section 7.7 in which discussions with experts during the question evaluation phase about the degree of subjectivity of the domain are examined. As for the *Dutch law* domain, no scores are visible as the study has been unable to have the domain evaluated. This is further discussed in Section 7.8.

In addition to Figures 6.2 and 6.3, the weighting difference of the number of evaluations across the domains can be seen through the measure of *count of domain question evaluations* in Table 6.3. Notably, the *business continuity* domain has a significantly larger number of evaluations than the other domains. This is a results of two factors: (1) it has the largest question count with 33 questions; and (2) its has been evaluated by the five experts. However, this provides significant evidence that the domain's value. Assessing its distribution of **usefulness** score, 90% are either **useful** or **very useful**, and 68% of the **ease of use** scores are either **easy** or **very easy**.

As a central concept of the framework, the *continuity guarantee* domain can see improvements in the study's confidence of the findings with more evaluations. Based on the score distribution from two interviews, for **ease of use**, 57% of the scores fall between **neutral** (26%) or **useful** (30%). As for the **usefulness** distribution, 97% of the scores are either **useful** or **very useful**.

The *data and application migration* has been evaluated in three interviews. The domain's scores fall more towards the **easy** and **useful** sides, with 63% of scores as either **easy** or **very easy**, and 81% as either **useful** and **very useful**. For the *testing* domain, from three interview evaluations, 81% of the **ease of use** scores are distributed between **difficult** (21%), **neutral** (25%), or **useful** (35%). Where as the **usefulness** scores fall toward the *useful* side, with 95% being either **useful** or **very useful**.

Regarding the *disaster recovery* and *service level agreement* domains, they have been evaluated in four and five interviews respectively. In both domains, for **ease of use** and **usefulness**, the scores are fall towards **easy** and **useful** sides. In the *disaster recovery* domain, 62% of scores are either **easy** or **very easy**, and 81% are **useful** or **very useful**. For the *service level agreement* domain, 75% fall are either **easy** or **very easy**, and 83% are **useful** or **very useful**.

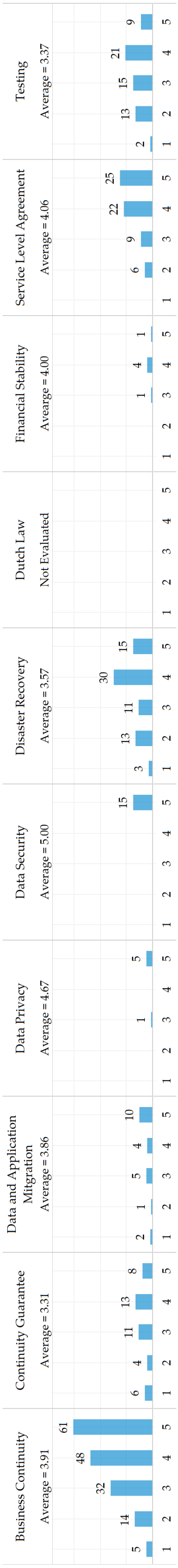


FIGURE 6.2: Domain **ease of use** score distribution in which a number of domains can bee seen with noticeable counts of low scores, indicating that there is some degree of difficulty in collecting evidence for the domains' questions

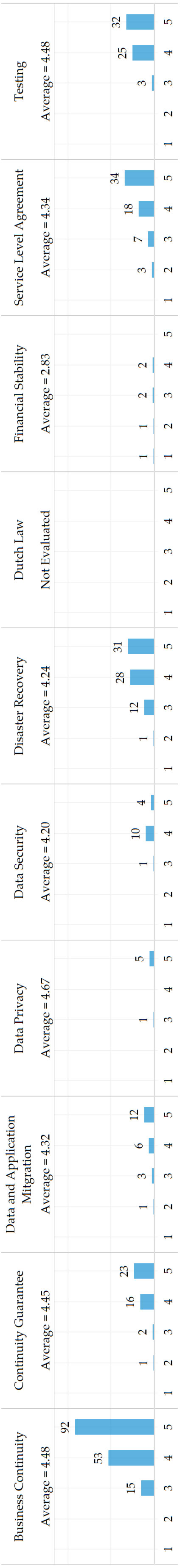


FIGURE 6.3: Domain **usefulness** score distribution in which the majority of scores are either useful or very useful, with only eight scores falling below neutral

The *data privacy* domain has only been evaluated once. As this domain consists of questions that have been created from the requirements for compliance with GDPR, it can be expected that additional evaluations may not change the value of the domain significantly. A similar stance is taken on the *data security* domain. Due to the high-level nature of the domain's questions in addressing compliance with existing standards, it is not expected that further evaluations would change the value of the domain significantly.

6.5.3 Question Level Findings

As previously mentioned, the **ease of use** criterion, while insightful, does not carry a strong impact on the overall value of the framework. As such, this sub-section will focus on highlighting findings pertaining to questions that have scored poorly in **usefulness** criterion. The only question to receive a **very useless** score resides in the *financial stability* domain, which has already been flagged for removal.

Addressing the questions that have been given a **useless** score, *CGU-02.12* has been evaluated twice, with one score of **useless** and another score of **very useful**. As previously mentioned, the *continuity guarantee* domain can be improved with more evaluations. More evaluations can resolve this unsurety cause by scoring situations like what has been seen in *CGU-02.12*. A similar situation can be seen in the cases of *DAM-02.1*, *DRE-04.03*, and *SLA-01.15*.

6.6 Qualitative Evaluation Results

To elicit qualitative information from the experts pertaining to the framework's **usefulness**, **operational feasibility**, **completeness**, and **ease of use**. Ten open-ended questions are asked in each interview. Nine questions have been formulated in a manner that can allow for a *yes* or *no* answers to be derived from the discussions of the questions. *Q-8* is an exception to this, as it has been intentionally structured to excite brainstorming sessions for the purpose of eliciting improvement ideas for the certification method currently applied. The experts are also encouraged to emphasize the reasoning for their answers to each question. The audio of interviews is not recorded. As such, the experts' responses are recorded by the researcher through note-taking, Allowing key insights to be extracted from the dialogue. Table 6.4, displays the results which are elaborated on in the following sub-sections.

6.6.1 Operational Feasibility Findings

Following the results from *Q-1*, all the experts found that the framework's design is easy to understand, with the only comment referring to re-structuring some questions to improve clarity. Such improvements occur either during or after the interviews as a question is identified as unclear. These modifications are recorded in the *change log* of the framework.

Q-2 has mixed results with five experts replying with *yes* and three with *no*. For the experts who answered *yes*, the primary concern is that if too many questions can be set as *not applicable*. Over usage of this answer option can result in inconsistencies across the assessed SaaS providers in terms of each assessment's thoroughness in addressing the different risk controls. This has to potential to degrade the value and trustworthiness of the framework's certification mark. Experts who answered

TABLE 6.4: Evaluation results from binary answer type open-ended questions addressing the degree of ease of use (EU), usefulness (U), operational feasibility (OF), completeness (C) of the framework

ID	Question	Criterion	I-1	I-2	I-3	I-4	I-5	I-6	I-7	I-8
Q-1	Do you find the design of the framework easy to understand?	OF	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Q-2	Should a limit be placed on the number of "Not Applicable" answers?	OF	Yes	Yes	Yes	No	Yes	Yes	No	No
Q-3	Do you see yourself or a colleague making using of this framework in the future?	OF	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Q-4	Are there any controls or questions that you believe are missing from the parts of the framework you reviewed?	C	Yes	Yes	No	Yes	Yes	Yes	Yes	No
Q-5	Are the options available in the answer satisfaction (answer input level) column appropriate for judging the question answers?	C	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Q-6	Is there anything else you would like to see included in the framework?	C	No	Yes	No	Yes	Yes	Yes	Yes	No
Q-7	Based on the questions you have reviewed, is there any question that if answered with "Not Satisfactory" or "Not Applicable" should result in the SaaS provider being disqualified from receiving any grade of certification mark?	U	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
Q-8	How would you determine the grade of certification mark based on the total score?	U	-	-	-	-	-	-	-	-
Q-9	Do you believe that different grades of certification mark should be awarded based on the resulting total score from the framework?	U	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Q-10	Do you think that only the SaaS provider should be assessed and why?	EU	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No

no, based their decision on the variability of requirements for SaaS providers across different SaaS industries.

For *Q-3*, experts that answered *yes* and are not from Europe, stated that it could be used to target European customers as a consulting tool. For countries outside of Europe, the *data privacy* domain may not be applicable, thus decreasing the domain's degree of generalizability. The decision to only address *data privacy* under GDPR is intentional as the framework's targeted stakeholders are European. The only expert to state *no*, based the response on the fact that at the moment he is only concerned with data security, and already uses a data security maturity model in his consultancy work.

6.6.2 Completeness Findings

The insights gathered from *Q-4* created a set of new requirements that have been adapted in the current version of the framework, as well as requirements for future versions due to the study's time restriction. From experts who answered *yes*, requests have been made for creating more granulated questions addressing user identity management testing, authorization testing, and roles and responsibilities of the different teams involved in executing business continuity plans. Interest has been expressed in including a domain that addresses the physical security controls of the organizations in the SaaS supply chain. One expert expressed interest in questions that assessed an organization's health. This has been attempted in the framework through the *financial stability* domain. However, it has been flagged for removal due to reasons discussed in Section 7.7. The *no* responses brought attention to the size of the framework as a potential hindrance to its professional use. The framework may seem daunting to complete due to the number of questions and time taken to complete it. A leaner version of the framework containing the most critical questions can be created to alleviate this hindrance. Such a version creates a quick pre-assessment tool for SaaS providers interested in becoming certified.

Q-5 addresses the answer input levels discussed in Section 5.4, for which the majority of experts answered *yes*. Two experts do not agree that the answer input options are appropriate. Both stating that the answer input levels need to be more clearly defined and the associated scores justified. This improves the decision-making process for selecting the correct answer level based on the evidence provided by the SaaS provider. Additionally, direct reference is made to the existing answer input levels' in-applicability to the data security domain questions. As a result, additions have been made to the answer input levels and are discussed in Section 7.2.

Those who answered *Q-6* with a *yes*, provided additional requirements for consideration. One would like to have access to a report that tracks the improvements of a SaaS provider from one assessment to another. This can be achieved in future versions by providing a report displaying the assessment scores for each domain over a period of time. Another expert expressed his interest in seeing if insights can be gathered on the SaaS provider's prioritization of RTO across applications and customers in the event of a widespread disruption event. Lastly, the need for physical security control testings is recommended if it is decided to include the physical security control domain in a future version of the framework.

6.6.3 Usefulness Findings

The majority of *Q-7*'s answers agreed that there are questions that should result in a SaaS provider being disqualified if one of the questions receive a low score. A number of questions, if scored low, provide indicate of critical vulnerabilities in the domain and the system as a whole. Due to the large number of questions being evaluated by most experts, they were unable to provide insights into all the questions that can be seen as critical indicators. Some questions have been flagged as critical. However, to confidently incorporate this feature into the framework is not possible at this moment. To ensure this is done correctly, more evaluations need to be conducted with more emphasis place on identifying critical questions. As for the expert who did not agree with this, bias might be present as he has recently developed a cannabis/ agricultural enterprise resource planning SaaS solution, called *Emisha*. As a SaaS provider, one can understand the hesitation to agree with the question as this feature increases the potential for disqualification. Potentially decreasing the SaaS provider's brand image if the public is made aware of the disqualification.

Q-8 has been formulated different, to avoid *yes* or *no* answers. This is intentionally done as an attempt to initiate brainstorming sessions to discover new methods for determining the certification mark. During the discussion, the current method used by the framework is explained, and the experts prompted to think of different methods. Six experts agreed that the current method used is satisfactory. However, two experts provided other options for consideration. Assigning individual weights to each question is suggested and investigated. Tweneboah-Koduah and Buchanan (2018) provides a suggestion in the form of determining the degrees of inter-dependency between systems and assigning weights based on the degrees. However, this is problematic when using quantitative methods for risk assessment as it has not been well explored by studies in the perspectives of cybersecurity risk assessment.

Q-9 has been unanimously agreed to by the experts. The use of different grades of certification marks creates the opportunity for SaaS providers to improve and achieve higher grades. Public displays of such progress can generate greater trust in the SaaS provider's brand. Greater trust has the potential to attract new customers who may have been hesitant prior to the public notice of certification improvement (Pauley, 2010).

6.6.4 Ease of Use Findings

Q-10's responses, despite being *yes* or *no*, all expressed interest in determining the degree that a SaaS provider is monitoring their SLAs with their service suppliers. *I-7* is the only expert to explicitly state that the SaaS provider is fully responsible as they are the ones that interact with the customers. Additionally, *I-2* expressed concern that the SaaS customers should also be assessed as the customer's security controls can create vulnerabilities that can potentially damage the SaaS provider. The only *no* answer is based on the reasoning that if a SaaS provider is using third-party services, those services should be assessed for vulnerabilities. This reason can be attributed to the expert's limitation of only evaluating the *data security* domain. Questions that addressed the monitoring of the SLAs with third and fourth parties appear in other domains.

Chapter 7

Framework Evolution

7.1 Introduction

This chapter discusses the major changes made to the framework. Major changes are identified as either additions or removals of framework elements. It is important to note that other minor changes have been made but are not mentioned here. Examples of minor changes are spelling corrections and re-structuring of questions to improve clarity. Table 7.1 shows the domain results after the removal of questions.

TABLE 7.1: Domain evaluation results after removal of questions, resulting in an overall **ease of use** average decrease by 0.02 & overall **usefulness** average increase by 0.03, with total question count of 125

Info: Max criterion average is 5, minimum is 1		**Evaluation Criterion**		
Risk Domain ID	**Calculation**	**Ease of Use**	**Usefulness**	**Notes**
Business Continuity	Sum of Criterion Scores	611	700	1 question removed.
	Count of Domain Question Evaluations	156	156	
	Criterion Average	3.92	4.49	
Continuity Guarantee	Sum of Criterion Scores	139	187	
	Count of Domain Question Evaluations	42	42	
	Criterion Average	3.31	4.45	
Data and Application Migration	Sum of Criterion Scores	85	95	
	Count of Domain Question Evaluations	22	22	
	Criterion Average	3.86	4.32	
Data Privacy	Sum of Criterion Scores	25	25	
	Count of Domain Question Evaluations	5	5	
	Criterion Average	5.00	5.00	1 question removed.
Data Security	Sum of Criterion Scores	40	34	
	Count of Domain Question Evaluations	8	8	3 questions removed.
	Criterion Average	5.00	4.25	
Disaster Recovery	Sum of Criterion Scores	257	305	
	Count of Domain Question Evaluations	72	72	Unable to get new question evaluated.
	Criterion Average	3.57	4.24	
Service Level Agreement	Sum of Criterion Scores	252	269	
	Count of Domain Question Evaluations	62	62	
	Criterion Average	4.06	4.34	
Testing	Sum of Criterion Scores	202	269	
	Count of Domain Question Evaluations	60	60	
	Criterion Average	3.37	4.48	
Financial Stability	Sum of Criterion Scores			Domain Removed. Not included in grand total.
	Count of Domain Question Evaluations			
	Criterion Average			
Dutch Law	Sum of Criterion Scores			Domain Removed. Unable to get domain evaluated.
	Count of Domain Question Evaluations			
	Criterion Average			
Grand Total	**Sum of Criterion Scores**	**1,611**	**1,884**	
	Count of Domain Question Evaluations	**427**	**427**	
	Criterion Average	**3.77**	**4.41**	

$$\text{Criterion average} = \frac{\text{Sum of Criterion Scores}}{\text{Count of Domain Question Evaluations}}$$

The decision to initiate changes based on evaluation findings from the interviews is primarily based on the quantity of information gathered in the interviews, and the time left until the next milestone date in the study's plan. For these reasons, the rounds of modifications contain differing numbers of interviews. The deletion of items only occurs at the end of the expert evaluation phase of the study, when the flow of new information from experts stopped.

All modifications to existing framework elements and new additions made to the framework are recorded in a *change log*, for which a snippet is displayed in Appendix C.4. In the *change log* within the framework, for each log an *Item ID*, *Item description*, *Item type*, *Change type*, *Change description*, *Date*, and *Reason* are recorded. By recording these elements, the logs are explained clearly and the degree of traceability is improved. Minor modifications to improve the readability of questions have been made but are not discussed in this paper, however details about these modifications can be found in the framework's *change log*.

7.2 Scoring Method Additions

As mentioned in Section 6.6.2, six experts agreed that the general approach to fulfilling the answer input method of the framework is appropriate. However, two experts have expressed concern that the answer input levels need to been more clearly defined. This required further exploration of literature, more specifically, the scoring methods used in similar frameworks. This section explores the findings associated with the scoring method adapted for the software as a service (SaaS) continuity control framework.

7.2.1 Answer Input Level Improvement

Tweneboah-Koduah and Buchanan (2018) provide a review of existing methods of assessing security risk exposure of critical systems. They present a number of methods used in risk assessment, some of which are already addressed by questions in the framework. However, they present a security control effectiveness index, as seen in Table 7.2 that is used as the basis for assigning answer input scores. The index is intended to be used when attempting to determine available countermeasures for protecting assets against threats, and quantifying their effectiveness.

To decide which score would be assigned, the details of the explanations for the control indexes of Table 7.2 were compared to the guidelines created for *satisfactory*, *partially satisfactory*, and *not satisfactory* seen in Table 5.4. As the highest achievable level, *satisfactory* requires the full score of 1.0. In the researcher's opinion, index 2's use of "Default controls" and "Some technical controls" align with the details of *partially satisfactory*'s guideline. When compared to index 3, it does not fully align as "Security screening in recruitment" is not a concept addressed by the framework. As such, *partially satisfactory* is assigned a score of 0.4. *Not satisfactory*'s guideline does not align with index 1, as it contains "Default controls". *Not satisfactory* requires that the concept is not formally characterized and understood, with no supporting processes implemented. It can be extrapolated that this lack of knowledge prevents the implementation of security controls.

TABLE 7.2: Control effectiveness index, extracted from Tweneboah-Koduah and Buchanan (2018)

Index	Control Index Explanation	Control Scale	Control Score
1	Default controls. No security screening in recruitment. No technical controls. No security training. No awareness programmes. No cyberinsurance and compliance certification.	Very weak controls	0.2
2	Default control measures. Some technical controls. No security screening in recruitment. No security training. No security awareness programmes. No cyberinsurance and compliance certification.	Weak controls	0.4
3	Default security controls. Some technical control measures. Security screening in recruitment. No cyber awareness programmes. No cyber insurance and compliance certification.	Average controls	0.6
4	Default security controls. Some technical control measures. Security screening in recruitment. Cybersecurity training and awareness programmes. No cyberinsurance and compliance certification.	Strong controls	0.8
5	Default security controls. Some technical control measures. Security screening in recruitment. Cybersecurity training and awareness programmes. Existence of cyberinsurance and compliance certification.	Very strong controls	1.0

7.2.2 Certification Grade Levels

With the incorporation of the knowledge gained from Najjar and Al-Sarayreh (2015) and Tweneboah-Koduah and Buchanan (2018) to create the framework's answer input levels, a set of thresholds for determining the grade of certification mark have been created. This has been done by combining explanations of the five maturity levels and the control effectiveness index. This has resulted in the descriptions and thresholds for the certification grades see in Table 7.3.

TABLE 7.3: Certification mark grades created by combining elements from Tweneboah-Koduah and Buchanan (2018) and Najjar and Al-Sarayreh (2015) to suit the context of this study

Grade	Certification Description	Threshold	Status
Very Weak	The implemented controls are not formally characterized and understood, with default technical controls, and no supporting processes.	20%	Not applicable
Weak	The implemented controls are formally characterized and understood, with default technical controls, minimum supporting processes.	40%	applicable
Average	The implemented controls are formally characterized and understood, with upgraded technical controls, and supporting processes described in procedures, tools and methods.	60%	Applicable
Strong	The implemented controls are formally characterized and understood, with advanced technical controls, and supporting processes implemented with quantitative quality and process performance objectives set for monitoring and managing.	80%	Applicable
Very Strong	The implemented controls are formally defined and managed using advanced technical controls and supporting processes partially aligned with best practices or standards with quantitative quality and process performance objectives set for monitoring and managing.	100%	Not applicable

Based on the certification descriptions created, only *Weak*, *Average*, and *Strong* are applicable to be used in the framework at this time. *Very Weak* is not appropriate as its requirements are too minimal to warrant a certification mark. *Very Strong* is not applicable because it sets a high standard that, realistically, the framework is unable to confidently guarantee at this time. To incorporate this, more evaluations and iterations of the framework need to be completed outside of this study.

7.3 SLA Domain Score Multiplier Addition

An algorithm has been derived from brainstorming sessions during interviews *I-2*, *I-3*, and *I-4* about the correlation between the value of the service level agreement (SLA) domain and the answers to questions *BCO-03.6* and *SLA-01.14*. It has been identified and agreed upon by the experts that the value of an SLA (in the context of this framework) depended on the answers to two questions: "Are supply chain entities (third & forth parties) monitored to ensure compliance with contractual agreements?", and "Does the SLA contain elements describing the compensation to the SaaS customer if the SLA is broken?". If a SaaS provider is not monitoring the compliance of its SLAs with other parties that its services depend on, the SaaS provider can not guarantee its compliance with promises made in its customer's SLAs. Additionally, if there is no compensation in the SaaS customer's SLA in the event that the SaaS provider breaks an agreement, there is little reason for the SaaS provider to abide to the SLA. Based on the two questions' answers, an SLA domain score multiplier (defaulted at a value of 1) is either decreased by one of two values, 0.2 or 0.4, or not changed. Inside the *Questionnaire report*, the SLA domain score subtotal is multiplied by the value of the SLA domain score multiplier. Resulting in the SLA domain score total which is added to the grand total score of the framework. The grand total score is used to determine the grade of the certification mark. The logic behind the algorithm used has been portrayed using the diagram in Figure 7.1.

Expert Evaluation of Decremental Values

To evaluate the algorithm and decremental values used, previously interviewed experts have been contacted. Each expert is provided with Figure 7.1 and asked, " Do you agree with the logic of the algorithm?" and "Do you agree with the values used in the algorithm that decrease the SLA domain score multiplier?" These discussions took place via online meetings, and their responses have been noted and are displayed in Table 7.4. Three of eight experts contacted responded.

TABLE 7.4: SLA domain score multiplier validation results for the algorithm's logic and the decremental values, in which a ✓ indicates an expert's agreement with an aspect of the algorithm's aspect

ID	Algorithm's Logic	Decremental Value = 0.2	Decremental Value = 0.4
I-2	✓	✓	✓
I-4	✓	✓	✓
I-7	✓	✓	✓

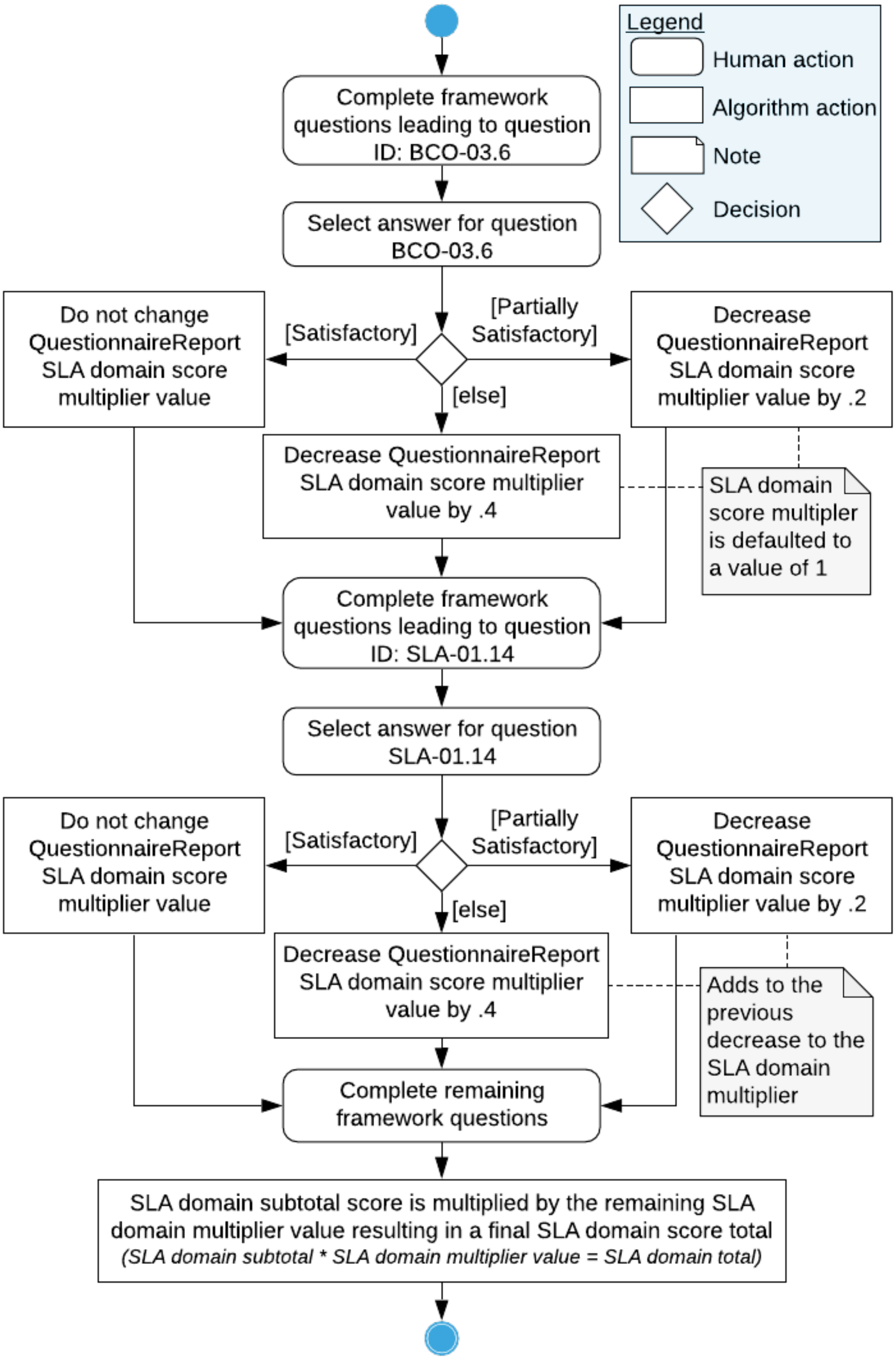
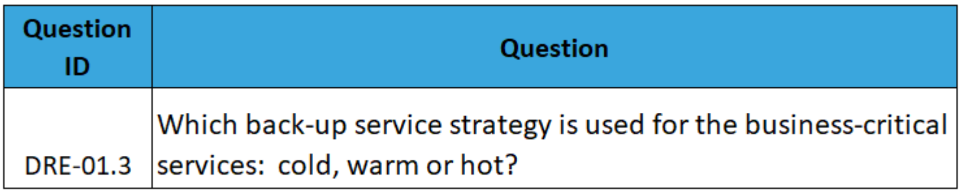

Legend
Human action
Algorithm action
Note
Decision
Complete framework questions leading to question ID: BCO-03.6
Select answer for question BCO-03.6
[Satisfactory]
[Partially Satisfactory]
[else]
Do not change QuestionnaireReport SLA domain score multiplier value
Decrease QuestionnaireReport SLA domain score multiplier value by .2
Decrease QuestionnaireReport SLA domain score multiplier value by .4
SLA domain score multiplier is defaulted to a value of 1
Complete framework questions leading to question ID: SLA-01.14
Select answer for question SLA-01.14
[Satisfactory]
[Partially Satisfactory]
[else]
Do not change QuestionnaireReport SLA domain score multiplier value
Decrease QuestionnaireReport SLA domain score multiplier value by .2
Decrease QuestionnaireReport SLA domain score multiplier value by .4
Adds to the previous decrease to the SLA domain multiplier
Complete remaining framework questions
SLA domain subtotal score is multiplied by the remaining SLA domain multiplier value resulting in a final SLA domain score total
(SLA domain subtotal * SLA domain multiplier value = SLA domain total)

FIGURE 7.1: Diagram describing the SLA domain score multiplier logic that impacts the overall weight of the SLA domain

7.4 Back-up Strategy Question Addition

During interview *I-6*, the expert brought attention to the importance of whether a hot, warm or cold back-up strategy is used. This topic has been further examined through literature and described in Section 4.3.1. The type of strategy determines the length of time before operations can resume. A cold back-up strategy may only replicate data on a periodic basis resulting in an RPO of hours to days (Suguna and Suhasini, 2014). Depending on the criticality of the application, this can be devastating and is the least effective strategy. As such, the question seen in Figure 7.2 has been added. Additionally, the answer options for this question are: hot, warm or cold. The resulting scores for the answers are: hot - 1 point, warm - 0.5 points, and cold - 0 points.



Question ID	Question
DRE-01.3	Which back-up service strategy is used for the business-critical services: cold, warm or hot?

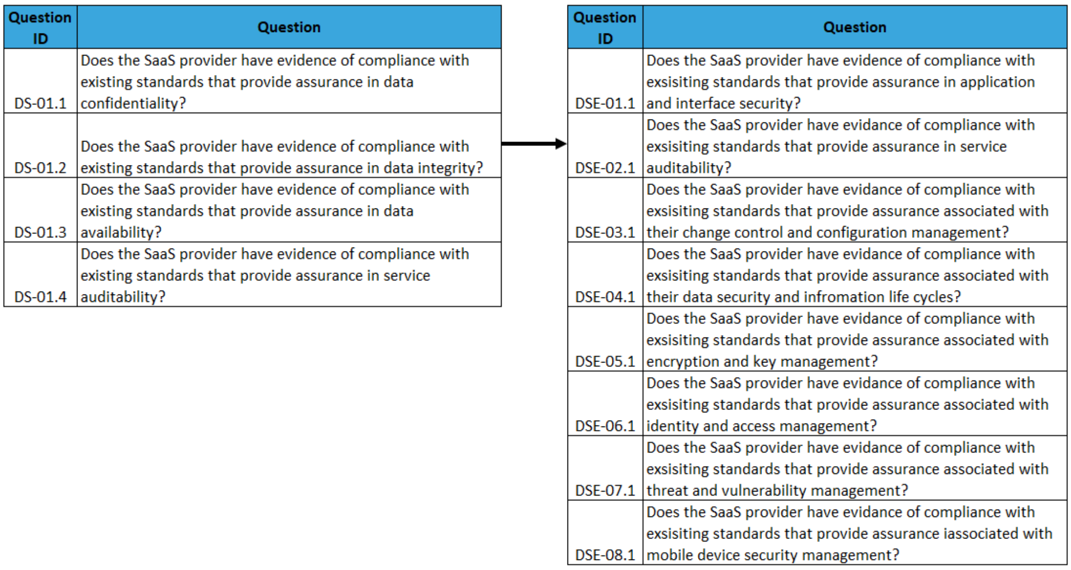
FIGURE 7.2: Back-up strategy question added to disaster recovery domain

7.5 Data Security Question Additions & Removals

In the first draft of the framework, the data security domain contained four questions that asked high-level questions requesting evidence for compliance with standards that support: data confidentiality, data integrity, data availability, and service auditability. It has been decided that more granulated questions are needed to gather more specific insights into the data security controls. Resulting in the enrichment of questions that request evidence for compliance with standards supporting: application and interface security, audit assurance and compliance, change control and configuration, data security and information life-cycle, encryption and key management, identity and access management, threat and vulnerability management, and mobile device security. These topics have been investigated in literature and described in Section 4.7, Table 4.5. These topics are inspired by the equivalent domains in the *Cloud Controls Matrix v3.0.1*. As the SaaS continuity control framework is focused on availability, asking a question about compliance with data availability standards is redundant, prompting its removal. The newly added questions address data confidentiality, data integrity, in a more granulated manner, the associated older questions addressing these topics are removed from the framework. Service auditability is not removed as no clear reason for removing it has been identified. These changes are visualized in Figure 7.3.

7.6 Business Continuity Question Removal

During *I-7*, a discussion about the redundancy of question *BCO-01.12* occurred. The set of questions displayed in Figure 7.4 addresses the risk control of conducting a business impact analysis, discussed in Section 4.2.1. However, question *BCO-01.12*

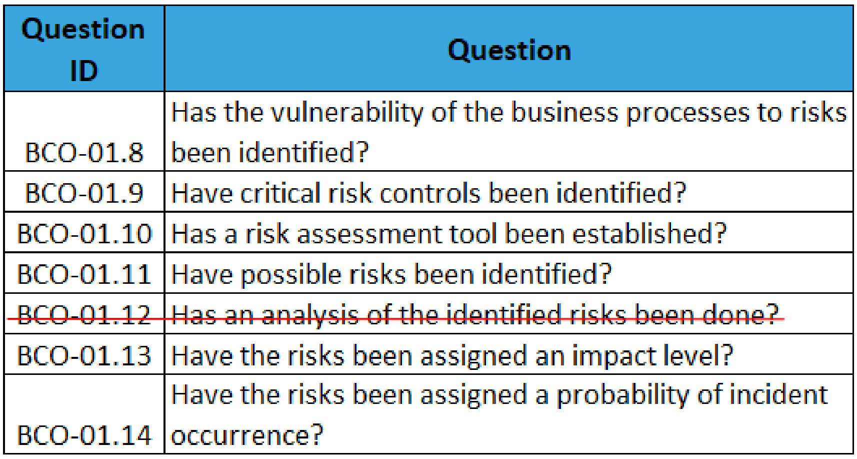


Question ID	Question
DS-01.1	Does the SaaS provider have evidence of compliance with existing standards that provide assurance in data confidentiality?
DS-01.2	Does the SaaS provider have evidence of compliance with existing standards that provide assurance in data integrity?
DS-01.3	Does the SaaS provider have evidence of compliance with existing standards that provide assurance in data availability?
DS-01.4	Does the SaaS provider have evidence of compliance with existing standards that provide assurance in service auditability?

Question ID	Question
DSE-01.1	Does the SaaS provider have evidence of compliance with exsisiting standards that provide assurance in application and interface security?
DSE-02.1	Does the SaaS provider have evidance of compliance with exsisiting standards that provide assurance in service auditability?
DSE-03.1	Does the SaaS provider have evidance of compliance with exsisiting standards that provide assurance associated with their change control and configuration management?
DSE-04.1	Does the SaaS provider have evidance of compliance with exsisiting standards that provide assurance associated with their data security and infromation life cycles?
DSE-05.1	Does the SaaS provider have evidance of compliance with exsisiting standards that provide assurance associated with encryption and key management?
DSE-06.1	Does the SaaS provider have evidance of compliance with exsisiting standards that provide assurance associated with identity and access management?
DSE-07.1	Does the SaaS provider have evidance of compliance with exsisiting standards that provide assurance associated with threat and vulnerability management?
DSE-08.1	Does the SaaS provider have evidence of compliance with exsisiting standards that provide assurance iassociated with mobile device security management?

FIGURE 7.3: Question additions and removals to the data security domain

asks if the analysis, which encompasses the steps addressed by the other questions, has been done. As the questions addressing the steps are asked, then *BCO-01.12* is redundant. Prompting its removal from the framework. The ordering of the questions has also been changed to match the order of the steps in a business impact analysis.



Question ID	Question
BCO-01.8	Has the vulnerability of the business processes to risks been identified?
BCO-01.9	Have critical risk controls been identified?
BCO-01.10	Has a risk assessment tool been established?
BCO-01.11	Have possible risks been identified?
~~BCO-01.12~~	~~Has an analysis of the identified risks been done?~~
BCO-01.13	Have the risks been assigned an impact level?
BCO-01.14	Have the risks been assigned a probability of incident occurrence?

FIGURE 7.4: Removal of question BCO-01.12 from business continuity domain due to redundancy

7.7 Financial Stability Domain Removal

As mentioned in Section 4.10, including financial stability as a certification criterion in the framework is discouraged by the expert participants in Schneider et al. (2014). However, the reasons behind the exclusion of financial stability are not discussed in

Schneider et al. (2014). The evaluations and discussions with interviewees, *I-4* and *I-7*, on the financial stability domain of the framework shed light on the reasons. Both interviewees encouraged the inclusion of the domain as the potential insights it can extract are valuable for SaaS customers. Unfortunately, it has been agreed upon by both interviewees that there is a high degree of subjectivity and complexity involved in determining a SaaS provider's financial stability.

For large SaaS providers, the interviewees mention that assessing the financial stability can be less subjective as large organizations have the resources and financial systems in place to conduct financial audits and reporting. This can reduce the workload required to compile the necessary financial statements for assessment. Depending on the criticality services provided by the SaaS providers, financial audits and reporting may occur on a regular basis due to government directives. For smaller and medium SaaS providers, it can be expected that their ability to conduct financial audits and reporting will be limited due to resource and maturity constraints. Based on discussions with the experts, it has been concluded that attempting to score small and medium SaaS providers on their financial stability using this framework will result in inaccurate results across the assessed organizations. This inaccuracy diminishes the value of the certification mark, thus negatively impacting the aim of the study. Additionally, it can not be expected that an information communication technology (ICT) professional using this framework will have the ability to make professionally sound interpretations of financial information. This is may not be an issue if the framework is applied using a team of personnel with different specializations (eg. financial analysis). Considering what has been mentioned, it has been decided to remove the entire domain from the framework.

7.8 Dutch Law Domain Removal

As mentioned in Section 4.11.1, the researcher acknowledges his lack of experience and understanding of the Dutch law system as the primary inhibitor to the development of the domain's questions. A Dutch lawyer has been searched for and upon initiating in dialogue regarding his contribution to the study, the lawyer's view is that the evaluation method is not suitable for the Dutch law questions of the framework. Furthermore, by the end of the evaluation phase of the study, this domain has not been evaluated. Thus, the domain can not remain in the framework's *questionnaire* and has been removed. However, during the evaluation phase further research was conducted in an attempt to improve the knowledge that can be applied to the Dutch law domain. Such an action is part of the *Rigor Cycle* of study's guidelines for conducting DSR by Hevner and Chatterjee (2010). The findings are applied to Dutch law questions and modifications are made as seen below:.

- *Does the SaaS provider declare Netherlands law applicable to the service and to any disputes about the service that may arise with customers?*

Based on the understanding developed through the reading of Regulation (EC) Rome I by Pöttering and Lenarčič (2008), this question is subject to the jurisdiction of the SaaS provider and SaaS customer, as well as the criticality of the services involved and contractual agreements made between the SaaS provider and SaaS customer. Such agreements can determine which law system will be applied to legal disputes. If both entities are registered as Dutch organizations, then Dutch private law is applicable. Some articles in Dutch private law are not mandatory and if this is the case, both entities can choose a different law system that is applicable on that particular legal dispute. If one of the entities is based outside the Netherlands, but inside an EU member state, Rome I is applicable. Article 3 of Rome I declares that entities can choose the law system they deem fit. If they do not choose one, article 2 and 4 of Rome I can be applied. In this instance, the law system of the country where the provider is based is applicable, regardless if the entities are registered in an EU member state or not. If both entities are not based in the Netherlands, but one of the entities is based in the EU, Rome I is applicable. If both entities are neither registered in the Netherlands nor in the EU, according to article 2 and 3 of Rome I, they can choose which law system is applicable. If they address a Dutch court the court will use article 3 and 4 of Rome I, in which the applicable law system is based on the jurisdiction that the SaaS provider is registered in.

The above creates a high level of subjectivity, as such, the question does not provide definitive insights into the level of risk related to the continuity controls offered by a SaaS provider. However, this question can be modified by addressing it to the Directive (EU) 2016/ 1148. Schulz and Korčok (2016, article 1) states that "this directive lays down measures with a view to achieving a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market." With such an objective, alignment with the directive can be seen as a positive indicator regarding risks involved within a jurisdiction's ICT industry. Therefore, the question can be replaced by one that is more generalizable, *"Does the law system of the jurisdiction that the SaaS provider is registered in, align with the articles described in Directive (EU) 2016/ 1148?"*

- *Does the SaaS provider comply with the statutory obligations, including the information obligations prescribed by articles 3:15d, 6:227b and 6:227c of the Civil Code?*

Articles 3:15d, 6:227b and 6:227c of the Civil Code are mandatory if the SaaS provider and customer are registered in Netherlands. If one of the entities is based outside the Netherlands but in the EU, Directive (EU) 2000/31 by Fontaine and Martins (2000) is mandatory. Within this directive, articles 13 and 14 state conditions for determining the liability of service providers in regards to the handling and modification of cached information, and hosting of information that has been deemed illegal. In Fontaine and Martins (2000), caching refers to the storage of information for the sole purpose of making the information's onward transmission to recipients more efficient. Where as, hosting refers to the storage of information provided by a recipient, If a SaaS provider adheres to this directive, the risk that it suffers financial or legal repercussions aligned with the directive is low. Thus the question can be modified to address Directive (EU) 2000/31, *"Does the law system of the jurisdiction that the SaaS provider is registered in, align with the articles described in c?"*

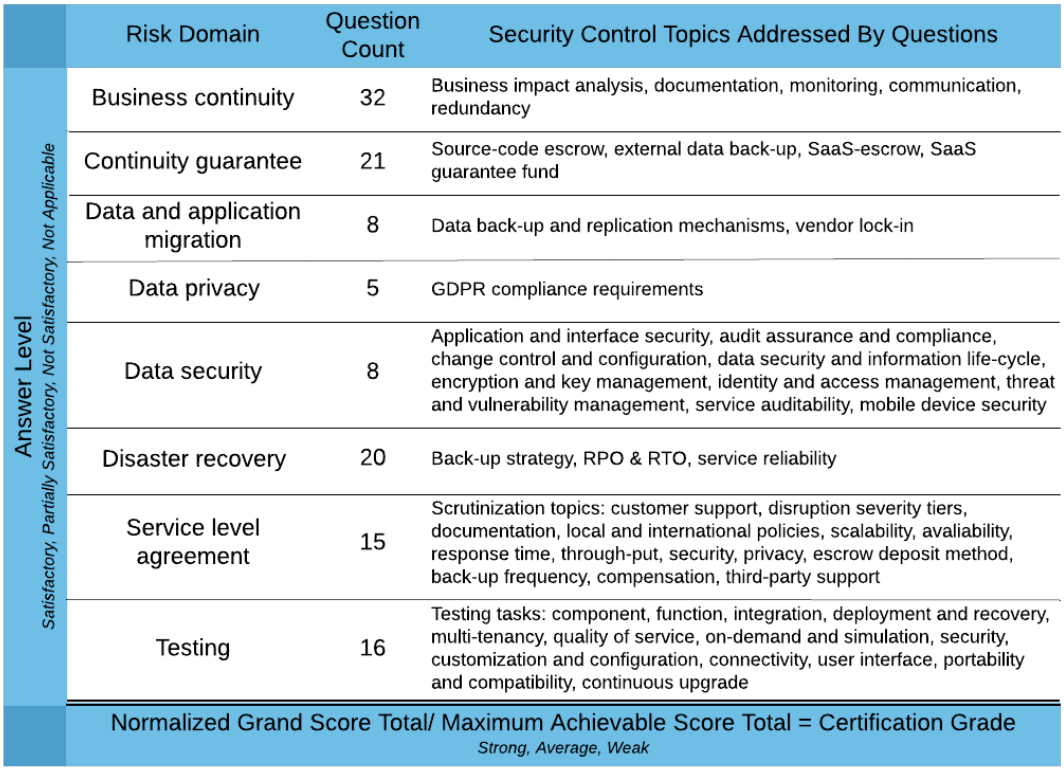
- *Does the SaaS provider supplies the service in a manner that ensures that customers can comply with the provisions of articles 47 to 53 inclusive of the State Taxes Act (Algemene Wet Rijksbelastingen)?*

It is evident that the researcher miss interpreted the above question which has been sourced from Zeker-Online (2019). As a result the question has been modified as follows, *"Does the SaaS provider comply with the provisions of articles 47 to 53 inclusive of the State Taxes Act (Algemene Wet Rijksbelastingen)?"*. Compliance with tax regulations is mandatory, as such this question still retains value as non-compliance can lead to financial and legal repercussions; such as fines and forced administrative dissolution of the SaaS provider.

Modified Questions Moved to User Guide
As discussed, there is perceived value in the modified versions of the questions, despite not being evaluated. It has been decided to place the questions in the framework's *user guide* as recommended considerations for public users of the framework.

7.9 Framework Overview

Figure 7.5 presents a general overview of the framework after the application of the additions and removals discussed in this chapter. It provides the final question count for each domain as well as the general topics that the questions address.



Answer Level

Satisfactory, Partially Satisfactory, Not Satisfactory, Not Applicable

Risk Domain	Question Count	Security Control Topics Addressed By Questions
Business continuity	32	Business impact analysis, documentation, monitoring, communication, redundancy
Continuity guarantee	21	Source-code escrow, external data back-up, SaaS-escrow, SaaS guarantee fund
Data and application migration	8	Data back-up and replication mechanisms, vendor lock-in
Data privacy	5	GDPR compliance requirements
Data security	8	Application and interface security, audit assurance and compliance, change control and configuration, data security and information life-cycle, encryption and key management, identity and access management, threat and vulnerability management, service auditability, mobile device security
Disaster recovery	20	Back-up strategy, RPO & RTO, service reliability
Service level agreement	15	Scrutinization topics: customer support, disruption severity tiers, documentation, local and international policies, scalability, avaliability, response time, through-put, security, privacy, escrow deposit method, back-up frequency, compensation, third-party support
Testing	16	Testing tasks: component, function, integration, deployment and recovery, multi-tenancy, quality of service, on-demand and simulation, security, customization and configuration, connectivity, user interface, portability and compatibility, continuous upgrade

Normalized Grand Score Total/ Maximum Achievable Score Total = Certification Grade

Strong, Average, Weak

FIGURE 7.5: Overview of the SaaS continuity control framework after additions and removals have been applied

Chapter 8

Case Studies

8.1 Introduction

Following the final improvements to the framework described in Chapter 7, two case studies have been conducted and evaluated using the strategy described in Section 2.4, and the case study protocol seen in Appendix B. As seen in section 2.4.1, in this multiple holistic case study, the framework is applied to small or medium Dutch software as a service (SaaS) providers during which the framework's questions are answered, continuity security control strengths and weakness are identified, and a certification mark determined. The framework is then evaluated by asking the SaaS provider open-ended questions that are derived from the *European Union Agency for Cybersecurity* (ENISA) certification scheme requirements listed in Section 3.10. General feedback from the SaaS providers and their answers to the evaluation questions are reflected on within the sections of this chapter.

8.2 Ex-post Evaluation Objectives

The framework is evaluated using an adapted definition of **effectiveness** from Prat, Comyn-Wattiau, and Akoka (2015). The study's definition of **effectiveness** is, "To what degree do insights gathered portray the level of risk associated with SaaS continuity controls?" To determine this degree, seven open-ended questions are asked to evaluate the framework's fulfillment of the certification scheme security objectives laid-out by *ENISA*. In addition to determining the degree of **effectiveness**, the questions aim to elicit further requirements, by promoting dialogue concerning missing concepts that are not explicitly asked by the existing questions, or generally not addressed. Similar to the expert evaluations, the representative of the SaaS provider is encouraged to engage in protocol analysis, discussing their thought process behind what they deem as interesting questions. Potentially generating new requirements for future versions of the framework. Importantly, as the researcher lacks the experience and knowledge to accurately interpret evidence presented to answer the framework's questions, the SaaS provider's opinions of what the answers should be, is used as the answers. During each session, information is noted by the researcher in the framework's *notes* area, as well as in an editable version of the case study guide.

8.3 Participating SaaS Providers

To provide a brief insight into the participating SaaS providers and their services, Table 8.1 provides a brief description of the SaaS solution, the role of the representative who participated, and the size of the organization. The cases have been pragmatically selected, by searching *LinkedIN* for organizations that meet the case study criteria and ideally provide impactful services to their customers.

TABLE 8.1: Information on participating SaaS providers

SaaS Provider	SaaS Solution Description	Representative's Role	Size
KindPlanner	Enterprise resource planning services for child care organizations providing functionalities such as, customer relationship management and invoicing.	CTO	Small
Channable	Data feed management and smart advertising automation services that create, optimize and export data feeds to over 2500 comparison websites, affiliated platforms and marketplaces. or generate ads for Google Ads and Microsoft Advertising.	CEO	Medium

In the following sections, each case study is discussed, revealing the insights gathered from the framework results, as well as any considerations that affect the recorded data. Figures 8.1 and 8.3 visualize the total awarded score, and total missed score as a percentage of the overall achievable score for each domain. The overall achievable score is reduced by the number of *not applicable* answers, thus accounting for situational factors of each SaaS provider that impact the performance of the domains. Figures 8.2 and 8.4 visualize the number of *not applicable* answers and other answer types.

8.4 Case 1: KindPlanner

KindPlanner's solution connects administration, internal groups, parents, and children to assist in the operational cycle of childcare organization (eg. kindergartens). It contains functionalities such as scheduling, accounting, and customer relations management to create a system that supports childcare planning, personnel planning, and parental communication. The main findings from the session with *KindPlanner* are discussed below.

KindPlanner receives a certification mark of **strong** by achieving 81% of the overall achievable score. Referring to Figure 8.1, three domains received a grade of **average**. Notably, the algorithm discussed in Section 7.3 contributes to this. The *service level agreement* domain's value has been decreased by 20% due to a *partial satisfactory* score awarded to question *BCO-03.06*, resulting in the domain's **average** grade. *Kindplanner* reported that they are motivated by the *service level agreement* domain's only *not satisfactory* question, to improve their service level agreement (SLA) document by including elements describing their SaaS-escrow solution. The performance of the *business continuity* domain is attributed to twelve *partially satisfactory* and three *not satisfactory* answers, representing 48% of the answers. Most notably, is their lack of any implemented risk assessment tools and strategic risk management options. These missing elements may indicate an inaccurate conceptualization of the degree of understanding of their identified risks. *KindPlanner* recently moved to the *Microsoft Azure* environment for hosting their SaaS solution. As a result, many *business continuity* and *disaster recovery* technical controls are cover for by the *Azure* services they have invested in. *KindPlanner* expressed satisfaction with the monitoring system and hot back-up service available through the environment.

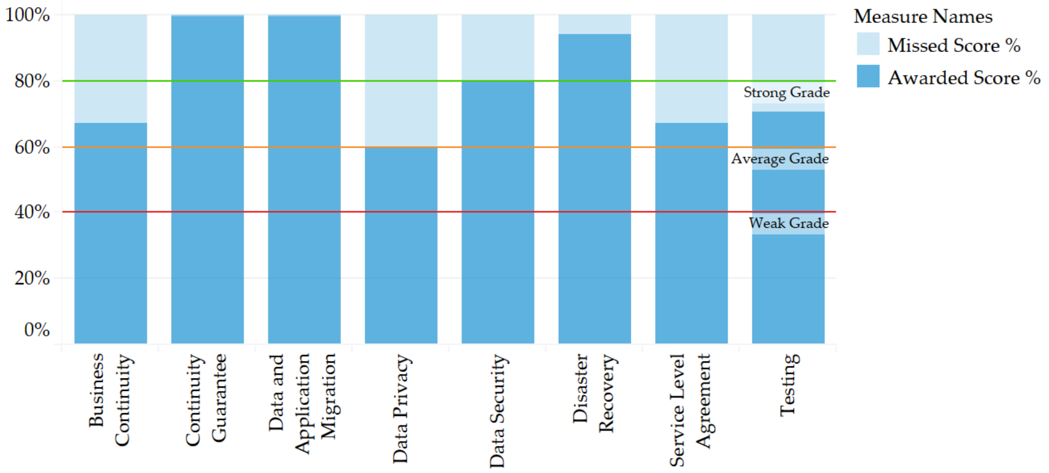


FIGURE 8.1: KindPlanner's domain score performance, with an overall certification mark grade of **strong** with *data privacy*, *business continuity*, and *service level agreement* achieving **average** grades

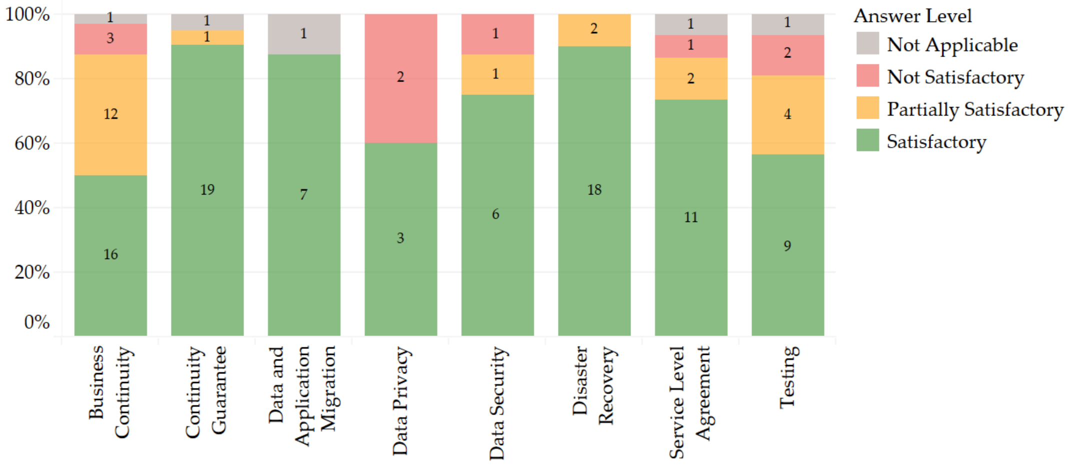


FIGURE 8.2: KindPlanner's answer level distribution, with a relatively high count of *partially satisfactory* answer in the *business continuity* domain, and a relatively high count of *not satisfactory* in the *data privacy* domain

8.5 Case 2: Channable

Channable collects data on the performance of their customer's products across over 2500 websites. The collected data is then provided to their customers for assessment, allowing them to create dynamic advertisements based on product demand

and supply. *Channable's* automated tools can then adjust the advertisements based on set parameters. Notably, *Channable* does not provide business-critical enterprise resource planning services. The impact of this and the resulting findings are discussed below.

Channable receives a certification mark of **average** by achieving 78% of the overall achievable score. Referring to Figure 8.3, two domains received a **weak grade**. As services offered by *Channable* are limited and do not exhibit high business criticality, an elaborate *continuity guarantee* has been deemed as unnecessary. Investing in *continuity guarantee* services does not improve their customer's business continuity situation in the event of a long term disruption or bankruptcy.

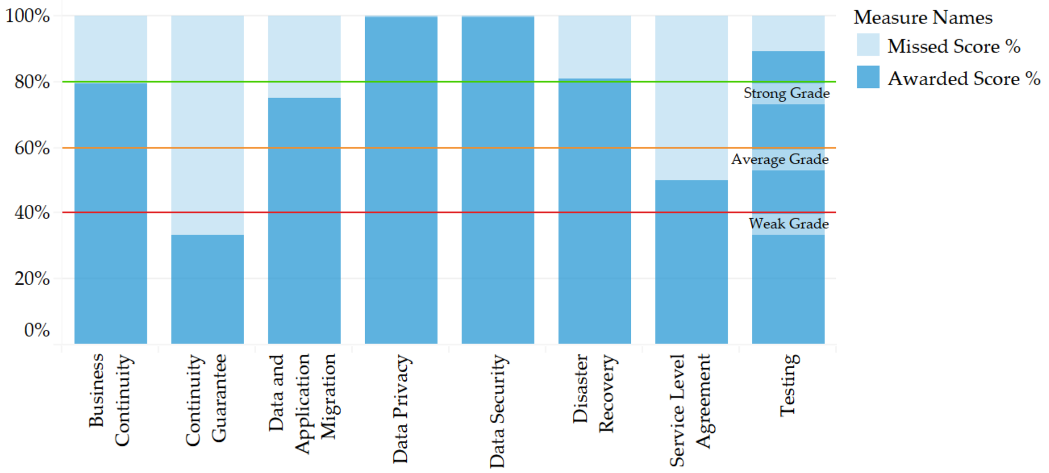


FIGURE 8.3: Channable's domain score performance, with an overall certification mark grade of **average** with *continuity guarantee* and *service level agreement* domains achieving **weak** grades

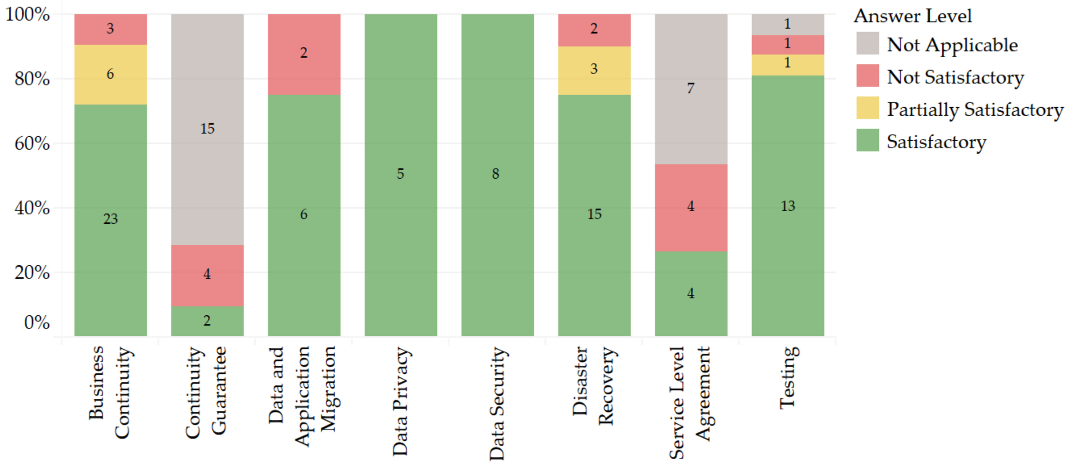


FIGURE 8.4: Channable's answer level distribution, with a relatively high count of *not applicable* and *not satisfactory* answers in the *continuity guarantee* and *service level agreement* domains

Channable has openly expressed that the nature of their services does not put their customers in a vendor lock-in situation. It is easy for their customers to gather their data in a .CSV format and migrate to a competitor. With this said, the high count of the *continuity guarantee* domain's *not applicable* answers can be understood as these mechanisms are not needed at this time, and the lack of them does not substantially increase the risk to their customers.

In the case of the *service level agreement* domain, the *not applicable* answer count is explained by the number of SLA document concepts addressed that exist in other contractual documents such as their *terms of use* and *data security policy*. As such, their lack of presence in the SLA document is not seen negatively, but can not positively influence the score of the domain. With that said, of remaining SLA document concepts addressed 50% are *not satisfactory*. This has highlighted missing key concepts that are in-fact part of *Channable's* sales pitch. They promote themselves as out-performing their competitors in these metrics. However, do not address them in their SLA document. *Channable* plans to adapted their SLA document and include the key missing concepts highlighted by the framework.

8.6 Effectiveness Findings

The questions used to evaluate the **effectiveness** of the framework as grounded in the security objective requirements from *ENISA* expressed in Barreira et al. (2019). After the all the questions are answered in the framework by the SaaS provider, the case study is concluded by prompting the SaaS provider to answer the questions seen in Table 8.2. Within the responses to these questions, new requirements can be elicited for improving the framework. It is important to note that the framework contains 125 questions, for which it can not be expected that the SaaS providers have remembered every concept that has been addressed. This may be a potential influence in their choice of answers.

TABLE 8.2: Framework effectiveness questions and answers from the SaaS providers who participated in the case studies

ID	Question	Kindplanner	Channable
E-1	Does the framework assess controls that protect stored, transmitted, or otherwise processed data against accidental or unauthorized destruction, loss or alteration, or lack of availability during the entire life cycle of the information communication technology (ICT) product, ICT service, or ICT process?	Yes	Yes
E-2	Does the framework assess controls that ensure authorized persons, programs, or machines are able only to access the data, services, or functions to which their access rights refer; to identify and document known dependencies and vulnerabilities?	Yes	No
E-3	Does the framework assess controls that record which data, services, or functions have been accessed, used, or otherwise processed, at what times and by whom?	No	No
E-4	Does the framework assess controls that make it possible to check which data, services, or functions have been accessed, used, or otherwise processed, at what times and by whom?.	No	No
E-5	Does the framework assess controls that verify that ICT products, ICT services, and ICT processes do not contain known vulnerabilities?	Yes	Yes
E-6	Does the framework assess controls that restore the availability and access to data, services, and functions in a timely manner in the event of a physical or technical disruption event?	Yes	Yes

Continued on next page

Table 8.2 - continued

ID	Question	Kindplanner	Channable
E-7	Does the framework assess controls that ensure that ICT products, ICT services, and ICT processes are secure by default and by design that ICT products, ICT services, and ICT processes are provided with up-to-date software and hardware that do not contain publicly known vulnerabilities, and are provided with mechanisms for secure updates?	No	Yes

E-1, *E-5*, and *E-6* have all been unanimously answered with *yes*. *E-1* and *E-6* both explicitly address the availability of services, which has been identified as the primary security area of focus for the aim of the study. Solidifying that the framework does effectively address security controls addressing the availability of services. *E-5* focuses on detecting vulnerabilities, which is a key concept of risk assessments. The framework contains questions that explicitly address the identification and analysis of vulnerabilities in the system. *E-3* and *E-4* have been issued unanimous *no* answers. The framework does not contain questions that address users as this level. This is a result of the high-level nature of the *data security* domain's questions. Further expansion of this domain can ensure that these concepts are explicitly addressed.

Channable's answer contradicts that of *KindPlanner* in *E-2* and *E-7*. For *E-2*, *Channable* justifies its decision by making a differentiation between authorized persons and correct persons. A security grouping of individuals may provide the members with authorization to access customer data. However, this does not mean that each of these members should be able to. A member may have access to data that they do not use in their role, thus not being the correct person to have access. This presents an opportunity for unnecessary access to sensitive data, widening an opening for potential threats, intentional and unintentional. Even though *E-7*'s answers differ, both parties agreed that the concepts addressed by the question are not explicitly asked in the framework. However, insights on the concepts can be extrapolated from the existing questions. *KindPlanner* flagged it as a difficult question as most of their developers use components that are available on the Internet. A question then arises, how does one know if the components have vulnerabilities? If a fault or vulnerability in these components is identified after the developers have implemented it, are the developers made aware of this in a timely manner, if at all? These are examples of questions that should be explicitly asked in the framework as it addresses the area of update deployment within the development life cycle.

8.7 Observations

The application of the SaaS continuity control framework in assessing *KindPlanner* and *Channable* has provided insights for the SaaS providers that have brought attention to potential improvements to their continuity controls. Additionally, the case studies has reveal new insights into the applicability of the framework. The potential implications of the insights are revealed below:

- Both SaaS providers have elicited new ideas for improvements to their controls, confirming that the framework can be a useful tool for self-assessment.

- The use of the *not applicable* answer option provides a degree of flexibility in regards to adjusting the scoring method to suit the context of the SaaS solutions.

- The concepts that are addressed in the *service level agreement* domain can exist in different documents. Prompting the consideration for modifying the domain to address *contractual documents*, including terms of use, data security policy, and other documents that describe obligations to the SaaS customer.
- Improvements to the clarity of some questions can be made by separating the current controls into smaller, more defined controls.
- Additional questions can be to the *data security* domain to satisfy the *ENISA* requirement questions that have been identified as not fully met in Section 8.6.

Chapter 9

Discussion

9.1 Introduction

As discussions of the findings and their implications from the expert evaluations and case studies have been discussed in Chapters 6, 7 and 8. This chapter is primarily aimed at examining the implications and challenges that have resulted from the process decisions made during the implantation of the design science research (DSR) methodology.

9.2 Design Science Research Adherence

The evaluation strategy adopted from Venable, Pries-heje, and Baskerville (2012), described in Chapter 2, prescribes an *ex-post* evaluation of the design process. To fulfill this, guidelines from Shrestha, Cater-steel, and Toleman (2014) for DSR evaluation is used, and the acceptance criteria for the multivocal literature review (MLR) by Garousi, Felderer, and Mäntylä (2019) is included.

9.2.1 Design as an artefact

This study has created a framework that can be used to assess the risk level associated with a software as a service (SaaS) provider's ability to continuity offering services during and after a disruption event. The design uses elements from the construction of maturity models from Bruin et al. (2005), while merging the definitions from Najjar and Al-Sarayreh (2015) for information communication technology (ICT) maturity levels with definitions of risk assessment scoring levels from Tweneboah-Koduah and Buchanan (2018). The resulting definition provides guidance for determining which answer input level to assigns to a question and the certification mark grade thresholds. These features are applied to the SaaS continuity control certification framework's 125 questions that address eight domains to identify risk assurance levels finally determining an overall certification mark.

9.2.2 Problem Relevance

The COVID-19 pandemic has forced the world to rely on SaaS services to communicate and conduct business using cloud ecosystems. Arguably, this forced shift to virtual and remote operations will not fade away completely. The ability of businesses to transfer over to SaaS solutions has its benefits and risks. The flexibility of employees to work from home or offices creates a blended work environment that has the potential to improve employee lifestyles. However, this creates a dependency on online services which can fall prey to a number of threats that can cause a variety of disruptions. Many advisory standards exist for *business continuity*, and its closely related domains. However, none of the freely accessible security frameworks assessed in this study address security controls for *continuity guarantees*, and contain the quantity of highly-granulated questions for *business continuity*, and *disaster recovery*, that is explicitly seen in the SaaS continuity control certification framework.

9.2.3 Design Evaluation

The evaluation method conceived of this study makes use of expert evaluations and multiple holistic case study methods. The expert evaluation method employed consists of two phases. The first, quantitatively assess the **ease of use** and **usefulness** of every question in the framework. During this phase, protocol analysis and brainstorming techniques are used to elicit qualitative data used to identify new requirements. The next phase collects only qualitative data using open-ended questions on **ease of use**, **usefulness**, **operational feasibility**, and **completeness**. Finally, the **effectiveness** of the framework is determined by conducting case studies and asking open-ended questions aligned with *European Union Agency for Cybersecurity's* (ENISA) requirements for certification schemes, such as security control certification frameworks. The combination of methods, techniques, and tools used through the evaluation of the framework has gathered a minimum of 556 direct data points, with no attempt being made to record the number of indirect contributions through discussions excited by protocol analysis and brainstorming. Systematic recording of indirect findings is not accounted for as the inclusion of these techniques occurred naturally in the expert evaluation phase.

Design Validation

The activities conducted in this study are aimed at evaluating the framework and are not seen as validations. To validate the framework, the application of the framework across multiple SaaS providers needs to be completed using a more thorough procedure than what has been applied in the study's case studies. Due to limitations in the researcher's ability to interpret evidence, most security control questions have been answered using the SaaS providers' opinions of what the answers should be. Ideally, this procedure should include a thorough investigation in which the user of the framework has working knowledge that enables a professional interpretation of evidence provided to be made. Following this, a series of check-ups need to be conducted over a set number of years to ensure that the risk assurance level awarded to the SaaS providers are accurate representations of their abilities.

9.2.4 Research Contributions

This study's *scientific contributions* begin with the formal identification and defining of the *continuity guarantee* concept, for which the framework has been constructed around. The *framework evaluation method* used has received positive feedback from this study's participating experts' experiences. On multiple occasions, experts have noted new ideas that are extracted from the questions in the framework as well as during the discussions prompted from the use of protocol analysis and brainstorming techniques. Experts who did not officially participate in the study, have also expressed interest in the evaluation method used, and its applicability in evaluating existing security frameworks. The resulting iterations of the framework have lead to the creation of a *unified modeling language (UML) class diagram* visualizing the structure of the framework and is seen in Figure 5.2. This diagram is a foundation that can guide the construction of future frameworks used by practitioners.

Additionally, the *LinkedIN strategy* used to acquire entities needed by the study has been explained and its process deliverable diagram (PDD) visualized in Section 2.4.1 and Appendix A.3, respectively. The number of connection requests sent using the strategy heavily outweighs the number of successfully completed expert evaluations. A quantitative view of the results discussed in Section 6.3, does not shine positively on the strategy. However, this strategy did acquire an acceptable number of evaluations while freeing up a valuable amount of time that is usually spent manually contacting potential participants. This freed-up time is used to review and improve the study multiple times as well as quickly reflect on the findings of the expert evaluations. The number of evaluations may have been higher if 15 messages from experts expressing interest in contributing were seen in a timely manner. Due to a management error, the researcher discovered these unaddressed messages at a late date. Additional benefits have also been seen through the numerous communications of interest by international SaaS organizations and researcher groups. With the globalization of professional social media platforms and low cost of operating on these platforms, researchers have the opportunity to market their research around the world. Contributing to a larger knowledge base and raising awareness of gaps in literature and practice.

Societal contributions of this study is evident in *SaaS continuity control framework* being publicly available for free download from the study's website, `www.saascontinuityframework.com`. This allows for the potential use of the framework as a foundation for a multitude of spin-off frameworks to be created and adapted. Adaptations can be made to suit different cloud contexts without the need to identify the main domains, a large number of their associated questions, and an appropriate evaluation method. Additionally, it can be used as a self-assessment tool for small and medium enterprises (SME) to determine the level of risk associated with their security controls and identify areas of improvement. Hopefully, achieving the aim of the study which is to foster improvements in risk awareness, and customer trust in SaaS, resulting in a healthier SaaS industry.

9.2.5 Research Rigor

The research process has been structured around the DSR methodology by Hevner and Chatterjee (2010), which has been shown to be suitable for the study. Furthermore, it has been enriched with a systematic literature review in the form of a MLR, allowing requirements to be elicited as described in Zave (1997), from grey and academic literature guided by the phases and acceptance criteria from Garousi, Felderer, and Mäntylä (2019). Following this, five evaluation criteria have been adapted from Prat, Comyn-Wattiau, and Akoka (2015), applied using a strategy guided by Venable, Pries-heje, and Baskerville (2012), and reported using a model derived from Shrestha, Cater-steel, and Toleman (2014). Then a multiple holistic case study has identified from Yin (1994) as a suitable means for testing the framework's alignment EU certification scheme requirement from Barreira et al. (2019). Lastly, compiling the study's methods, techniques, and tools using method engineering concepts from Brinkkemper (1996).

This study can be seen as evidence of the ability of scientific methods prescribed through literature to create an artefact based on domain knowledge acquired from literature, that can be used in a process that identifies and assesses real-world problems. The development of this study's artefact has resulted in an accumulation of concepts that provide a base for extrapolating insights into a SaaS provider's situation. This is used in an evaluation process to determine the degree of risk associated with their continuity controls, reveal improvement opportunities to the provider, and gather enough knowledge on the SaaS provider's system to allow the framework's user to provide additional improvement recommendations. This foundation of this ability lies in the domain and requirements process theories. Domain theory starts with preliminary modeling of a meta-schema of domain knowledge, which is abstracted, and used to model classes of information that can be specialised by applying further knowledge from different views on each domain (Jarke et al., 1993). The requirements process theory then uses the domain knowledge as building blocks to specify processes at several granularity levels while extracting the semantics of the processes' activities.

9.2.6 Design as a Search Process

The process of identifying relevant concepts, electing valid questions addressing these concepts, and ensuring that the questions have value, occurs iteratively throughout the MLR and expert evaluations. On occasion, newly found concepts from the expert evaluations are researched using the MLR process, then discussed in the study, to finally decide whether or not they should be addressed the framework. Close to 44% of the GL failed the quality assessment, providing indication of the effectiveness of the MLR's quality check process and the acceptance criteria applied.

9.2.7 Communication of Research

The structure of the study's paper, primarily the abundant use of tables, lists, and figures easily highlights the sources of the features and questions seen in the framework. Providing improved transparency into the evolution of the framework. The framework has dedicated features to ensure that it can be easily understood and used by practitioners. Its dashboard contains a number of interactive graphs and a table that provide insights into the results of the framework's *questionnaire*. Highlighting areas of interest, further assisting practitioners in the task of reviewing the results with stakeholders.

9.3 Validity Threats Mitigation

Table 9.1 provides an overview of the tactics used to minimize the degrees of threat caused by the four threats to validity, namely, construct validity, internal validity, external validity, reliability, and conclusion (Wohlin, 2014; Runeson and Höst, 2009; Ampatzoglou et al., 2019). There are many sub-threats within these five categories, however to address each sub-threat is unreasonable for this degree of study. As such, these five main categories can be seen as the parents most sub-threats and have been used in a large number of studies. These threats are discussed and issues examined later in this section.

Construct validity refers to the degree to which this study measures what it claims to measure. The study's adherence to the DSR guidelines, examined in Section 9.2, ensures that the methodology's cycles are iterated multiple times along with numerous elements that support the traceability of design decisions. The use of

TABLE 9.1: Validity threat mitigation tactics

Research Method	Tactic	Construct	Internal	External	Reliability	Conclusion
General Process	Adherence to DSR guidelines	✓			✓	
	Recording changes in framework's change log				✓	
	Evaluation of performance using score averages and score distribution via histograms					✓
Multivocal Literature Review	MLR guideline adherence	✓		✓		
	Applying GL quality check protocol	✓	✓			
	Employing data collection form		✓		✓	
Expert Evaluation	Interviewing 8 domain experts		✓	✓		
	Capturing expert insights from 5 countries			✓		
	Employing protocol		✓		✓	
Multiple Holistic Case Studies	Completing 2 case studies	✓	✓	✓		
	Capturing insights on non-business critical and business critical SaaS solutions			✓		
	Employing protocol		✓		✓	

MLR guidelines and the application of the tool seen in Appendix D.1 to adhere to the grey literature (GL) quality check process, ensures that the knowledge and requirements acquired, met the set quality standards. However, the selection of the search terms seen as attributes in Figure 1.1, can be enhanced by an initial grounding the selection in existing cloud computing taxonomies, such as Dutta, Peng, and Choudhary (2013). This would improve the effectiveness and efficiency of the MLR to elicit framework requirements. Additionally, use multiple interviews and case studies ensures that the information collected is supported by multiple expert opinions. Ideally, more interviews and case studies will strengthen these migration tactics. However, its must be acknowledged that this study is limited by its available manpower (1 researcher) and time frame (8 months).

Internal validity is the extent to which a piece of evidence supports a claim about cause and effect, within the context of this study. Degrees of restraint have been applied to the depth and quantity of the questions for in the influential domains outside of the core domains of: *business continuity*, *disaster recovery*, and *continuity guarantee*. Scoping the framework in such a manner improved the strengths of the core domains. While the other domains are addressed, there exists the possibility that the domains are generally missing concepts or not explicitly addressed by questions. As mentioned in previous chapters, the *data security* domain is important, but contains a large depth and quantity of concepts that the study is unable to thoroughly address at this time. This is mitigated by the high-level nature of the domain's questions. Furthermore, the peer-reviewing and piloting of the interview and case study protocols assist the study in its attempts to extract its desired insights. Notably, it is the researcher's belief that there is a degree of misinterpretation in the experts' understandings of the study's definition of the *ease of use* criterion scored during the expert evaluations. Due to the size of the framework, fatigue has been experienced during the expert evaluations. This has been mitigated by splitting lengthy evaluations into two sessions. This has been done in the case of *I-2*, *I-4*, *I-6*, and *I-7*. Notably, there is an unbalanced number of evaluations conducted on the domains. The final version of the *data privacy* and *data security* domains have only been thoroughly evaluated once, whereas, *continuity guarantee* has only been evaluated twice.

External validity is the degree of which the conclusions of this study can be applied outside of its context, across other situations, people, stimuli, and times. As the framework is aimed at small and medium sized SaaS providers, it may not contain all the elements valuable to larger enterprises. It does provide a foundation for expanding its depth of coverage, creating a catalyst for the potential to be applied in other situations. The use of an MLR to elicit requirements allows the study to acquire knowledge that may not be readily available in academic literature. All concepts are have been reviewed through the experts evaluations and case studies. Of which, the participants reside in five different countries, namely, Netherlands, Belgium, U.S.A, India, and Australia. Ensuring that besides the General Data Protection Regulation (GDPR) data privacy requirements, the framework's concepts are generalizable. However, it must be stated that in its current form, this framework is not applicable to the other layers of the cloud service layer seen in Figure 3.1.

Reliability is concerned with to what extent the data and analysis are dependent on the specific researchers and the degree of decision traceability. By adhering to the DSR guidelines, some degree of research bias is mitigated. This is also improved by the use of an MLR, which allows the capturing of both academic and practitioner insights. The need of an MLR has been validated by answering questions for determining the necessity for an MLR presented in Garousi, Felderer, and Mäntylä (2019). The diverse and heterogeneous nature of the GL accessed is not subject to traditional academic peer-review processes and creates a threat to validity in the form of researcher bias (Kitchenham, 2004). To mitigate this threat, guidelines for conducting an MLR are followed to ensure the credibility of the GL used (Adams, Smart, and Huff, 2017). The steps taken in the MLR have been clearly detailed in Section 2.2, and records kept enabling traceability of the decisions made throughout the study. However, the protocol for the MLR states that at least two researchers should conduct the quality assessment and code the literature (Garousi, Felderer, and Mäntylä, 2019). This could not be done as this study is conducted by only one researcher, and the supervisor can not be involved in the critical path of the study. Researcher bias is also addressed in the peer-reviewing of the protocols used in the study. The changes to the research context conceptual-model seen between Figures 1.1, 3.5, and 4.8, as well as the framework's *change log* enhances the traceability between the iterations of the DSR sub-cycles, and resulting design decisions. An overview of the resulting framework is seen in Figure 7.5.

Conclusion validity in this study pertains to the degree that the insights acquired from a statistical analysis of the quantitative criteria used in scoring the domains and questions are reasonable considering the data collected (Ampatzoglou et al., 2019). The major issue arises from the differing number of evaluations conducted on the domains and the number of questions within each domain. The use averages and score distributions at the domain and question levels, has been used to ensure that a clear idea of the performance of each domain and question can be extrapolated. The averages are useful for highlighting and making decisions on domains or questions that have many data points. The use of histograms to assess the score distribution, provides another point of view providing a catalyst of understanding as to how an average is calculated, and replace the use of an average as an assessment tool when there are too little data points.

9.4 Lessons Learned

This section serves as a personal reflection on the successes and challenges encountered during the study. It is the hope of the researcher that future researchers can gain insights that will allow them to avoid mistakes and improve their studies by enhancing successful elements of this study. The main points are ranked below in order of importance, with the first being the most important lesson:

1. **Find a study partner(s) that will work on their thesis alongside yours.** Doing this creates countless opportunities for brainstorming and quick peer-reviews. Having different points of view on how to tackle challenges will improve the creativity of the solutions employed. Ultimately, improving the quality of your work and reducing researcher bias in an unofficial capacity. This working relationship will provide motivation and create an outlet for venting when the frustration builds.

2. **Create a detailed research approach.** A detailed research approach will create more confidence in yourself, reveal unknown weak points in your study, and create an overall more grounded study. Later in the study, the time spent on this will reward you.

3. **Market yourself and your study.** This is a great opportunity to build your brand before entering the work force. Additionally, the attention you get from professionals can create instances where they help you out by providing networking assistance, advice, or even literature you may not be aware of.

4. **Besides the grade, set your own internal learning objectives.** Identify the opportunities in your study that can be beneficial to you outside of academia. Once those are achieved, everything else is value added. This will also motivate you as it creates a sense of personal reward for the hours you spend working on it.

5. **Be very explicit with your supervisor about your preferred style of communication and develop a type of informal social contract.** As an example, I sent periodic messages that simply inform my supervisor of the happenings in the study. State that these messages do not need responses, but only act as a manner of keeping them informed. Sometimes you may bring up a topic that excites them. It is your study and you are responsible for managing their interest in your work. This plays on the concepts of client engagement and expectation management.

6. **Try to make internal meetings more enjoyable.** This highly depends on the personalities of the research team, but developing internal humour between you and your supervisor will make meetings more enjoyable. The personality types of the people you work with and how they mesh together, impacts the maximum productivity level of the team as a unit.

Chapter 10

Conclusion

10.1 Introduction

The aim of this has been to *improve* the transparency of the software as a service (SaaS) industry *by* designing and evaluating a certification framework *that can* be used to analyze SaaS continuity control risks, and award certification marks to SaaS providers, *in order to* foster improvements in risk awareness and customer trust in SaaS. To determine if this is achieved, the set of research questions formulated in Section 1.1.2 are reflected on. This study is then concluded, with a discussion about future research opportunities that have revealed themselves during this study.

10.2 Research Questions

MRQ: Can a framework be created that portrays the level of risk associated with SaaS continuity controls by analyzing a SaaS provider's ecosystem including the methods, tools, and processes used to support these controls?

To reveal the answer to the main research question (MRQ), the study's process of answering the sub-research questions (SQ) is examined and findings expressed. These insights provide an indication of how well the study achieved its objectives.

SQ1: What framework design features are best suited for scoring the risk associated with SaaS business continuity controls?

These features have been formally drafted and discussed in Chapter 5. Following this, Chapter 6 evaluates the relative criteria of **operational feasibility** and **ease of use**. Finding that experts deem the features appropriate for achieving the aim of the framework. Following the insights gains through the expert evaluations, enhancements are made to the framework in the form of additions, removals, and modifications discussed in Chapter 7. Overall, the framework has been seen by experts as intuitive and easily understandable for a practitioner to use, while providing the necessary means for scoring risk.

SQ2: What business functions/ processes that support SaaS continuity controls should be analyzed in the certification framework?

The requirement elicitation activities needed to answer this question are seen in Chapter 3 and Chapter 4. The **usefulness** of these findings as questions in the framework is then evaluated and gaps identified in Chapter 6. With the help of expert insights, enhancements are made to clarify existing questions, while additions and removal made are discussed in Chapter 7. The resulting framework is put to the test in Chapter 8, in which SaaS providers are assessed using the framework. These cases studies elicit new requirements for the framework that can be applied in future expansions.

SQ3: What SaaS continuity guarantee specific concepts should be analyzed in the certification framework?

Following the same process described in SQ2's answer, the study has attempted to form a **complete** set of concepts specific and related to *continuity guarantees*. Identified gaps have been filled within scope of the study. However, some gaps have been revealed and discussed in Chapter 8. The main gaps primarily reside in the *data security* domains, which has been flagged as being out-of-scope for the study to address at a more granulated level. Based on the **effectiveness** findings related to the security area of availability, of which this study is focused on, the framework has been deemed **effective** at assessing the risk level associated with the domains.

SQ4: What is a suitable scoring and evaluation method for the certification framework to correctly assess security controls?

Based on the feedback from the experts in Chapter 6, the scoring and evaluation method has been deemed suitable. The details of these methods have also been based in the works of Najjar and Al-Sarayreh (2015) and Tweneboah-Koduah and Buchanan (2018). Combing elements of maturity models and risk assessments.

SQ5: What entities in the SaaS supply chain should be assessed?

In Chapter 3, the responsibilities of the supply chain entities are determined by looking at the degree of control over the technology and services SaaS customers purchase. Therefore, it has been decided that the SaaS provider, as the entity with the most control, should be assessed. However, experts have voiced their opinions that other entities, such as the SaaS customer should be assessed as they create security vulnerabilities that can threaten the SaaS provider. This view is correct, but the inclusion of this entity or other supply chain entities, increases the cost of applying the framework, potentially creating a situation in which SMEs can not afford the framework. Preventing the study from achieving its aim.

SQ6: What are suitable criteria and requirements for evaluating the framework?

This has been identified by referring to the taxonomy presented in Prat, Comyn-Wattiau, and Akoka (2015), and adapting the definitions of its criteria to the context of the study. Additionally, requirements for security frameworks aiming to certify cloud service providers (CSP) have been adopted from *European Union Agency for Cybersecurity* (ENISA), and applied to determine the framework's degree of alignment.

10.3 Future Research

Many ideas have been conceptualized during this study. As such, it is important to discuss those ideas which are rich enough to warrant the attention of future research projects.

Further Development of Framework

Referring to the insights gathered from Chapter 6, additional domains can be added to the framework as well as the addition of more granulated questions. A new domain addressing *human resources* can be added as this plays a vital part in the operations of any organization. A sub-par recruiting process can create vulnerabilities if newly recruited employees' abilities and backgrounds are not vetted for potential future security issues. Additionally, the *physical security* measures at the locations of the SaaS providers play a role in preventing malicious insider-attacks and infrastructure damage from occurring. Finally, the existing *data security* domain can be easily expanded on by enriching it with controls and questions from the existing framework, improving the quality of the risk assurance associated with the framework's certification mark. However, such actions will expand the time required to complete an assessment, and the cost of the certification mark. Such efforts can make use of tools such as the *devils quadrangle*, see in Figure 10.1. It consists of four main dimensions, namely, time, cost, quality, and flexibility, that are used as indicators for monitoring of modifications, and investigations to evaluate the resulting changes to the framework (Pourshahid et al., 2007). For clarification, flexibility can be seen as the framework's ability to assess security controls in different system contexts (eg. business-critical or not critical). Whereas quality is equivalent to this study's definition of effectiveness.

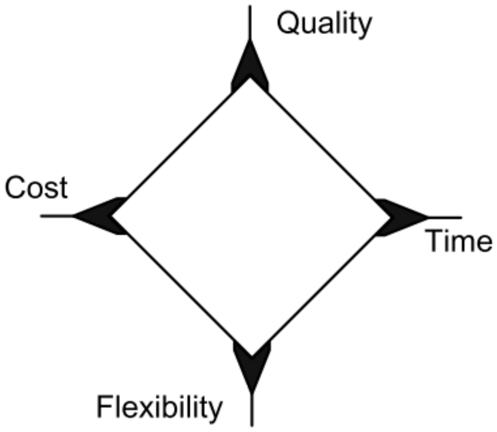


FIGURE 10.1: Devil's quadrangle for monitoring and investigation of modifications to artefacts and processes, extracted from Pourshahid et al. (2007, p.4)

Another option to compensate for increases in the size of the framework is the creation of leaner versions of the framework that are associated with each certification mark grade. A leaner version can contain a lower quantity of questions, selected based on a more extensive evaluation of their usefulness. Decreasing the time and cost to SaaS providers that are aiming to achieve certification marks that have a lower risk assurance level. Additionally, the frameworks that represent the next level of risk assurance can be provided ahead of time to SaaS providers to allow for self-assessments to be completed. Essentially providing a set of improvement steps that may potentially encourage the provider to return for future certifications. The leaner framework idea has been elicited from the expert evaluations discussed in Chapter 6.

Inter-dependency of Risk Security Controls in a System

Tweneboah-Koduah and Buchanan (2018, p.1394) state, "[that] the interface between critical infrastructure and their inter-dependencies has not been well explored by extant studies in the perspectives of cybersecurity risk assessment." Thus, identifying a gap in research for which this study arguably falls into. Section 7.3 provides a documented and evaluated attempt at adjusting the SLA domain's overall value based on the answer to a question in the business continuity domain, and a question within the SLA domain. Figure 7.1 visualizes the inter-dependencies between two security control questions, and the perceived degrees of dependency that impact the value of an SLA. SLAs can be seen as an infrastructural element within cloud security controls, as it can contain contractual obligations for service level in terms of confidentiality, integrity, and availability. Further research into the development of methods for assigning degrees of inter-dependencies between security controls, and the questions that assess them, the accuracy of the risk assessment can be improved. Figure 10.2 visualizes system dependencies through a causal loop diagram describing key variables affecting a system's performance, and behavioral changes.

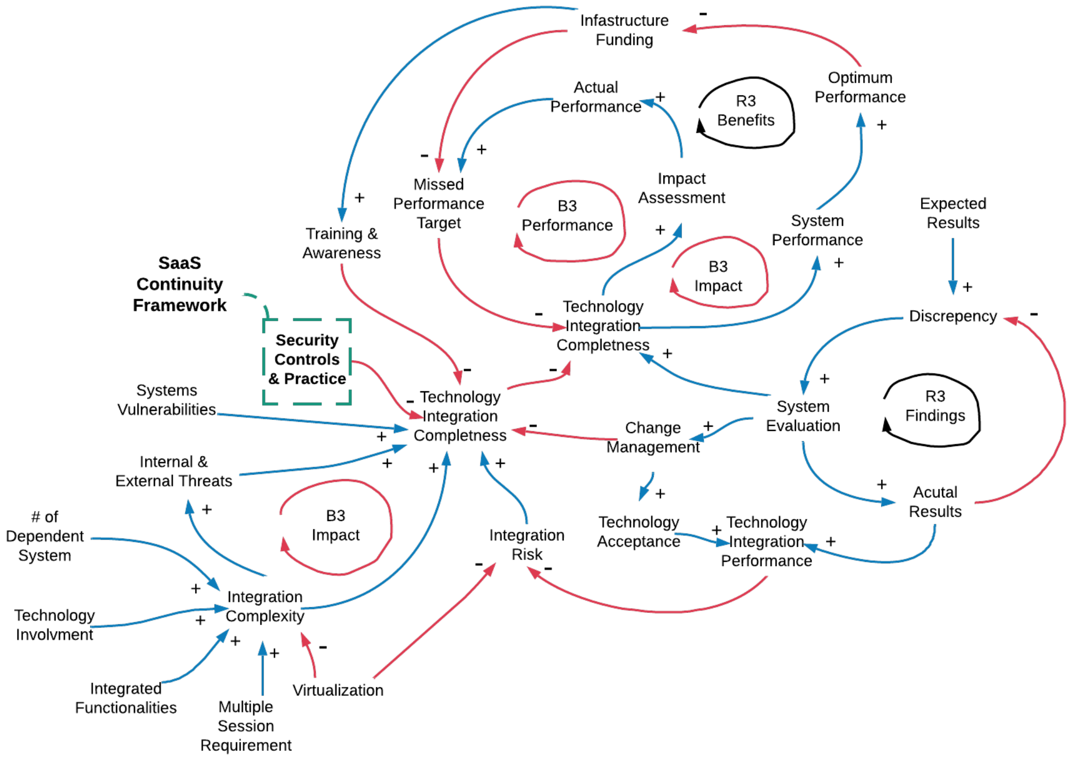
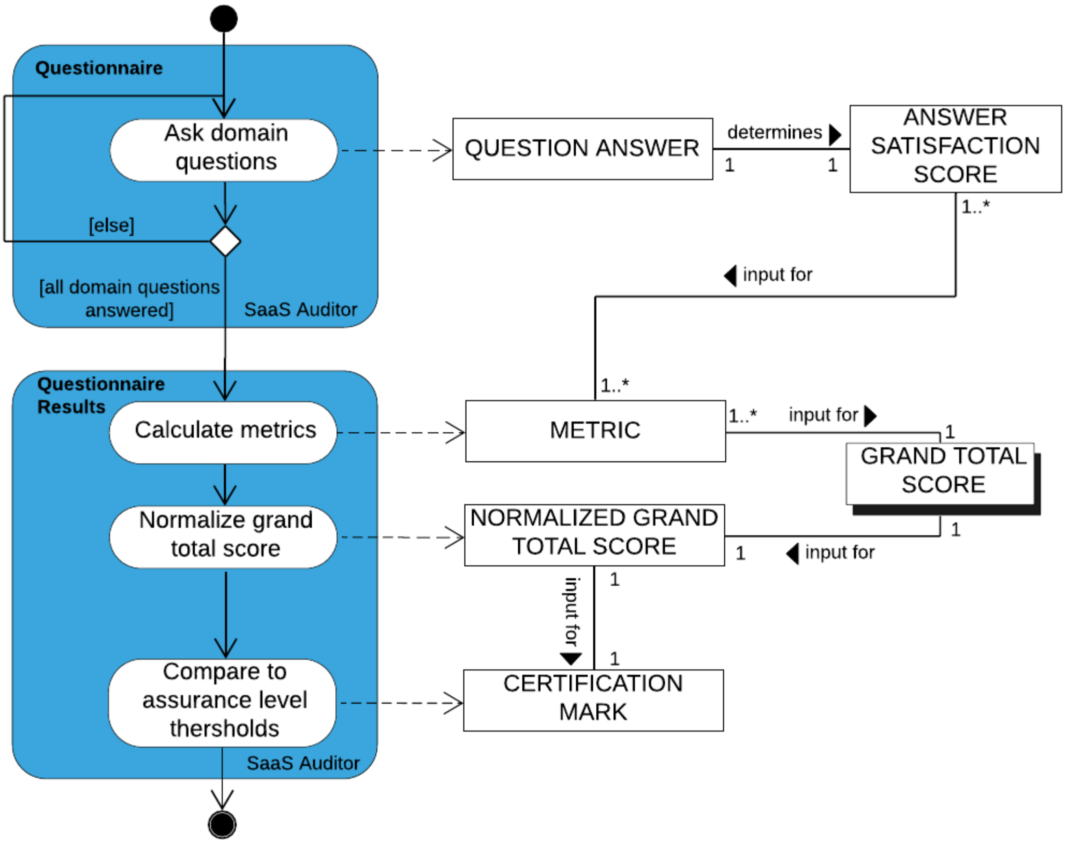


FIGURE 10.2: Causal loop diagram of inter-dependencies between system infrastructures proposed in Tweneboah-Koduah and Buchanan (2018, p. 1398), in which the **SaaS continuity control framework** determines the degree of risk associated with the security controls and practice factor (green square), affecting the technology development risk factor. "The technology deployment risk: This is the system's security risk exposure due to technology deployment. It is a function of the sum of the system's vulnerabilities, threats events, integrated induced complexities divided by available (active) [security controls], and security practices (eg. training and awareness). It is assumed that the higher the rate of [security controls], the lower the overall deployment risk."

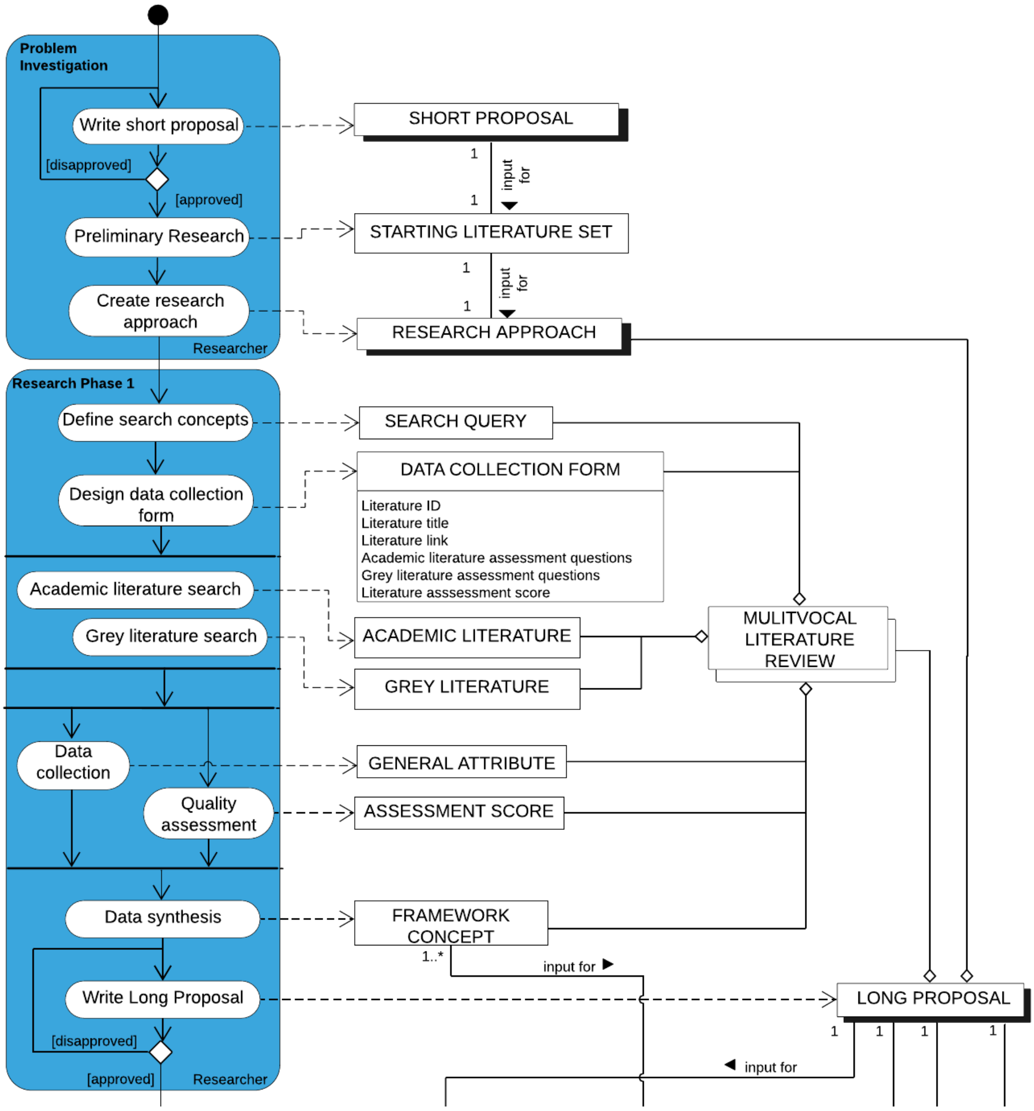
Appendix A

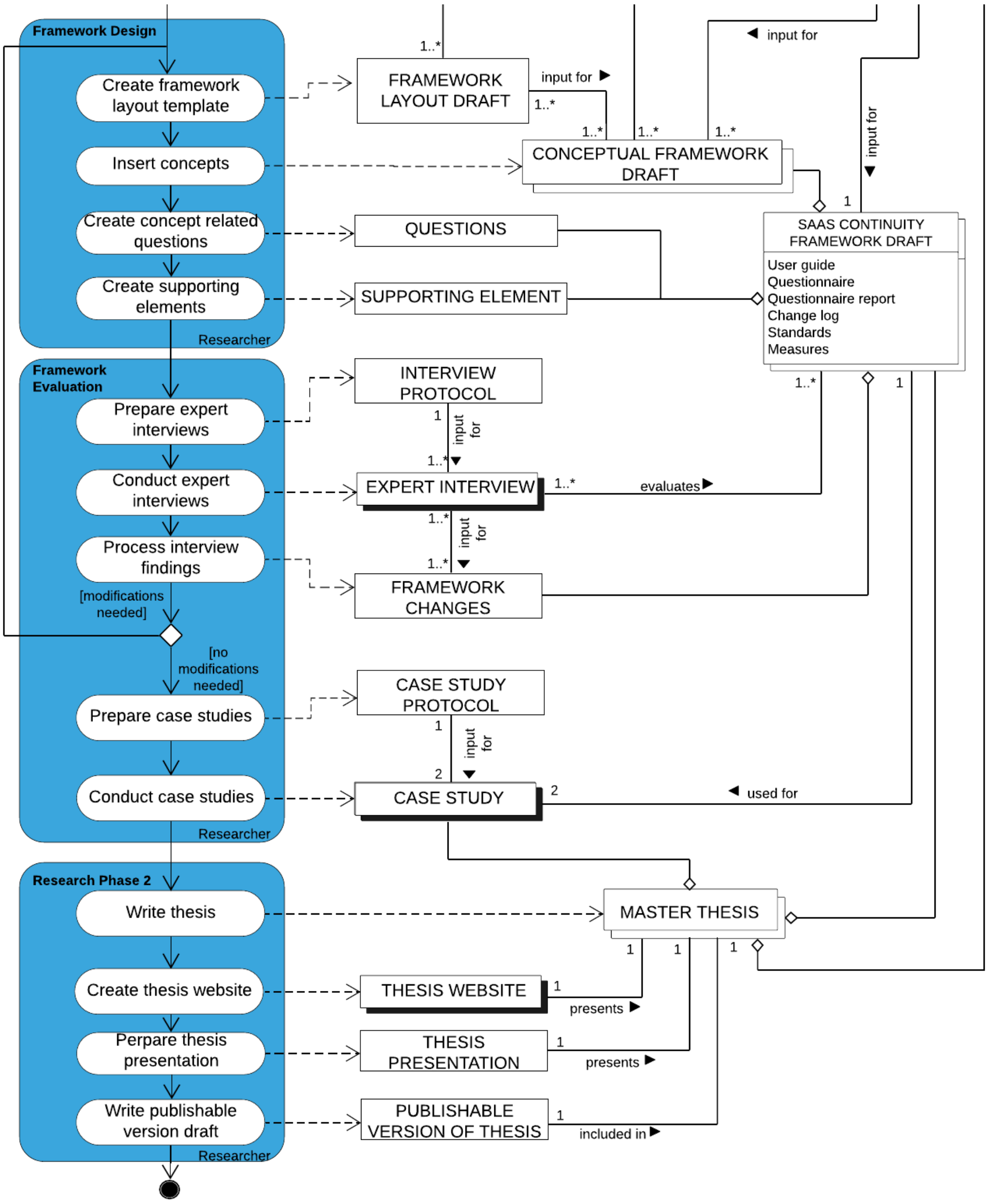
Process Deliverable Diagrams

A.1 Framework Operational Procedure

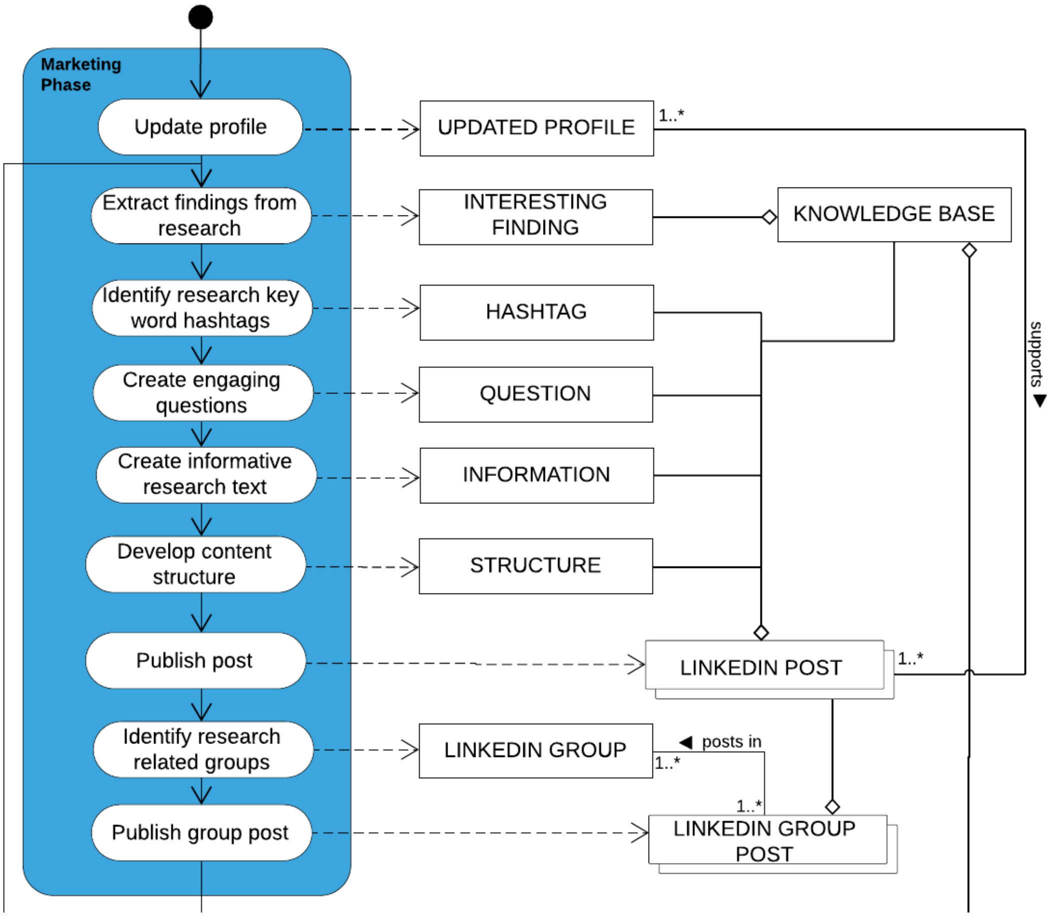


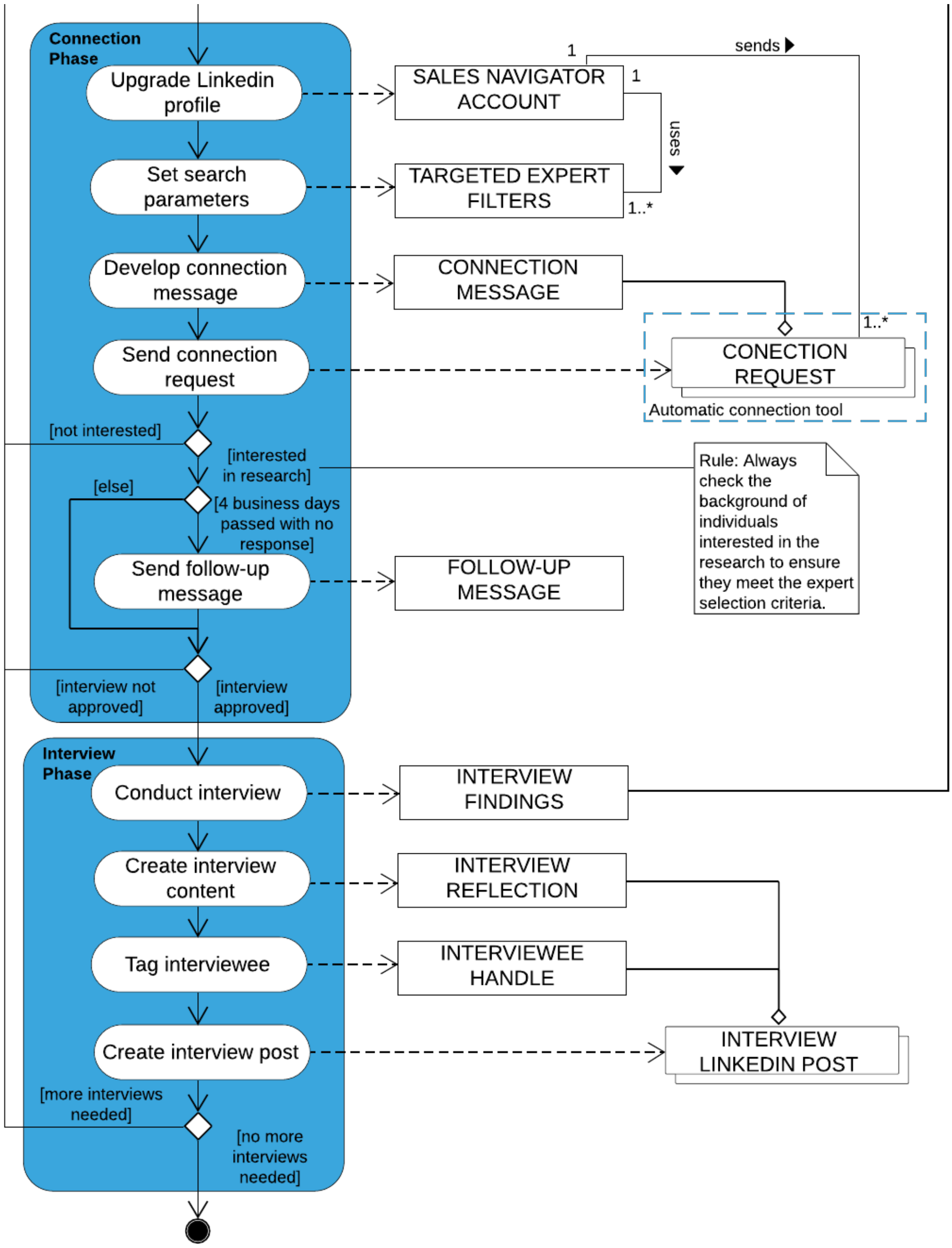
A.2 Study Approach




Framework Design
Create framework layout template
Insert concepts
Create concept related questions
Create supporting elements
Researcher
Framework Evaluation
Prepare expert interviews
Conduct expert interviews
Process interview findings
[modifications needed]
[no modifications needed]
Prepare case studies
Conduct case studies
Researcher
Research Phase 2
Write thesis
Create thesis website
Perpare thesis presentation
Write publishable version draft
Researcher
1..*
FRAMEWORK LAYOUT DRAFT
input for
1..*
1..*
1..*
1..*
input for
CONCEPTUAL FRAMEWORK DRAFT
input for
1
QUESTIONS
SUPPORTING ELEMENT
SAAS CONTINUITY FRAMEWORK DRAFT
User guide
Questionnaire
Questionnaire report
Change log
Standards
Measures
INTERVIEW PROTOCOL
1
input for
1..*
EXPERT INTERVIEW
1..*
evaluates
1..*
1
1..*
input for
1..*
FRAMEWORK CHANGES
CASE STUDY PROTOCOL
1
input for
2
CASE STUDY
2
used for
MASTER THESIS
1
1
1
THESIS WEBSITE
1
presents
THESIS PRESENTATION
1
presents
PUBLISHABLE VERSION OF THESIS
1
included in

A.3 LinkedIN Approach

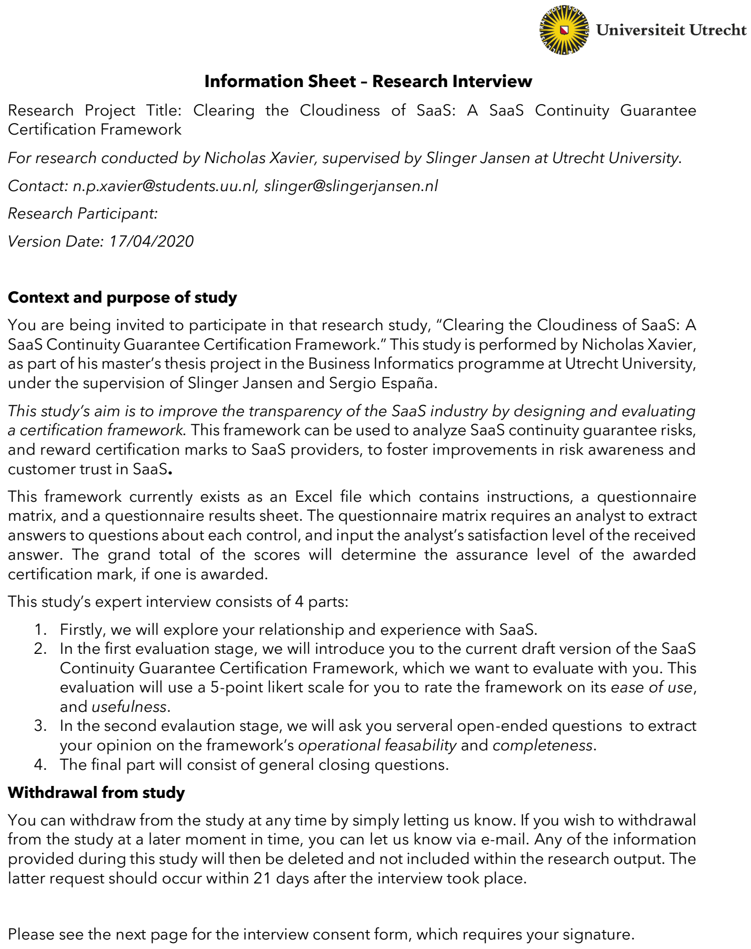



Connection Phase
Upgrade Linkedin profile
Set search parameters
Develop connection message
Send connection request
[not interested]
[interested in research]
[else]
[4 business days passed with no response]
Send follow-up message
[interview not approved]
[interview approved]
Interview Phase
Conduct interview
Create interview content
Tag interviewee
Create interview post
[more interviews needed]
[no more interviews needed]
SALES NAVIGATOR ACCOUNT
TARGETED EXPERT FILTERS
CONNECTION MESSAGE
CONECTION REQUEST
Automatic connection tool
FOLLOW-UP MESSAGE
INTERVIEW FINDINGS
INTERVIEW REFLECTION
INTERVIEWEE HANDLE
INTERVIEW LINKEDIN POST
sends
uses
1
1
1..*
1..*
Rule: Always check the background of individuals interested in the research to ensure they meet the expert selection criteria.

Appendix B

Interview & Case Study Documents

B.1 Interview Research Information Sheet



Universiteit Utrecht

Information Sheet – Research Interview

Research Project Title: Clearing the Cloudiness of SaaS: A SaaS Continuity Guarantee Certification Framework

For research conducted by Nicholas Xavier, supervised by Slinger Jansen at Utrecht University.

Contact: n.p.xavier@students.uu.nl, slinger@slingerjansen.nl

Research Participant:

Version Date: 17/04/2020

Context and purpose of study

You are being invited to participate in that research study, "Clearing the Cloudiness of SaaS: A SaaS Continuity Guarantee Certification Framework." This study is performed by Nicholas Xavier, as part of his master's thesis project in the Business Informatics programme at Utrecht University, under the supervision of Slinger Jansen and Sergio España.

This study's aim is to improve the transparency of the SaaS industry by designing and evaluating a certification framework. This framework can be used to analyze SaaS continuity guarantee risks, and reward certification marks to SaaS providers, to foster improvements in risk awareness and customer trust in SaaS**.**

This framework currently exists as an Excel file which contains instructions, a questionnaire matrix, and a questionnaire results sheet. The questionnaire matrix requires an analyst to extract answers to questions about each control, and input the analyst's satisfaction level of the received answer. The grand total of the scores will determine the assurance level of the awarded certification mark, if one is awarded.

This study's expert interview consists of 4 parts:

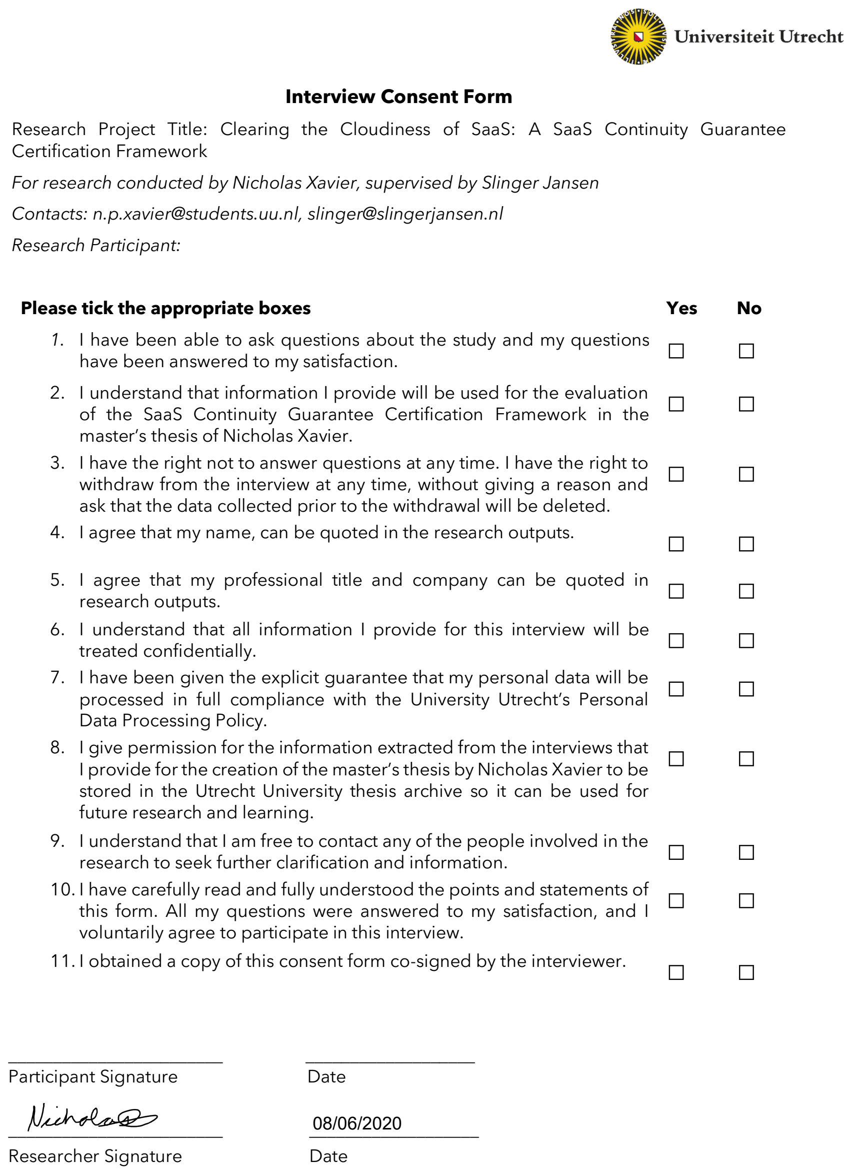
1. Firstly, we will explore your relationship and experience with SaaS.
2. In the first evaluation stage, we will introduce you to the current draft version of the SaaS Continuity Guarantee Certification Framework, which we want to evaluate with you. This evaluation will use a 5-point likert scale for you to rate the framework on its *ease of use*, and *usefulness*.
3. In the second evalaution stage, we will ask you serveral open-ended questions to extract your opinion on the framework's *operational feasability* and *completeness*.
4. The final part will consist of general closing questions.

Withdrawal from study

You can withdraw from the study at any time by simply letting us know. If you wish to withdrawal from the study at a later moment in time, you can let us know via e-mail. Any of the information provided during this study will then be deleted and not included within the research output. The latter request should occur within 21 days after the interview took place.

Please see the next page for the interview consent form, which requires your signature.

B.2 Interview Consent Form



Universiteit Utrecht

Interview Consent Form

Research Project Title: Clearing the Cloudiness of SaaS: A SaaS Continuity Guarantee Certification Framework

For research conducted by Nicholas Xavier, supervised by Slinger Jansen

Contacts: n.p.xavier@students.uu.nl, slinger@slingerjansen.nl

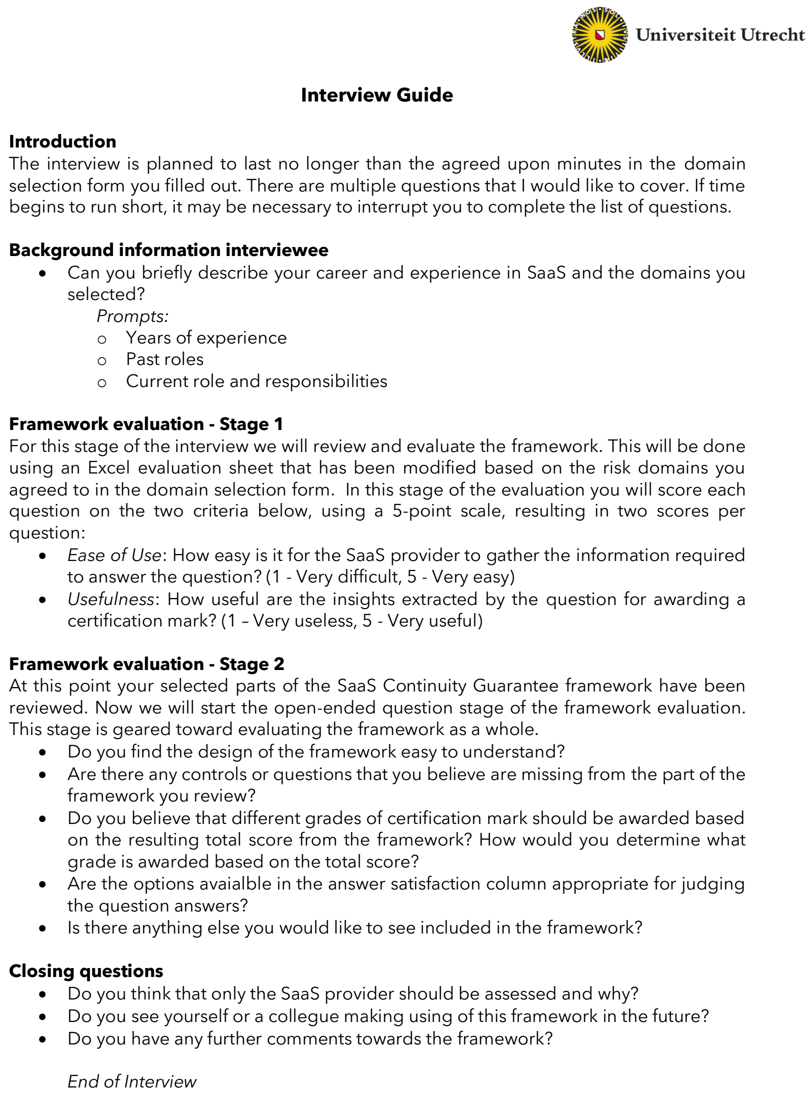
Research Participant:

Please tick the appropriate boxes	**Yes**	**No**
1. I have been able to ask questions about the study and my questions have been answered to my satisfaction.	□	□
2. I understand that information I provide will be used for the evaluation of the SaaS Continuity Guarantee Certification Framework in the master's thesis of Nicholas Xavier.	□	□
3. I have the right not to answer questions at any time. I have the right to withdraw from the interview at any time, without giving a reason and ask that the data collected prior to the withdrawal will be deleted.	□	□
4. I agree that my name, can be quoted in the research outputs.	□	□
5. I agree that my professional title and company can be quoted in research outputs.	□	□
6. I understand that all information I provide for this interview will be treated confidentially.	□	□
7. I have been given the explicit guarantee that my personal data will be processed in full compliance with the University Utrecht's Personal Data Processing Policy.	□	□
8. I give permission for the information extracted from the interviews that I provide for the creation of the master's thesis by Nicholas Xavier to be stored in the Utrecht University thesis archive so it can be used for future research and learning.	□	□
9. I understand that I am free to contact any of the people involved in the research to seek further clarification and information.	□	□
10. I have carefully read and fully understood the points and statements of this form. All my questions were answered to my satisfaction, and I voluntarily agree to participate in this interview.	□	□
11. I obtained a copy of this consent form co-signed by the interviewer.	□	□

______________________ ______________________
Participant Signature Date

Nicholas 08/06/2020
Researcher Signature Date

B.3 Interview Guide



Universiteit Utrecht

Interview Guide

Introduction

The interview is planned to last no longer than the agreed upon minutes in the domain selection form you filled out. There are multiple questions that I would like to cover. If time begins to run short, it may be necessary to interrupt you to complete the list of questions.

Background information interviewee

- Can you briefly describe your career and experience in SaaS and the domains you selected?

  Prompts:
  - Years of experience
  - Past roles
  - Current role and responsibilities

Framework evaluation - Stage 1

For this stage of the interview we will review and evaluate the framework. This will be done using an Excel evaluation sheet that has been modified based on the risk domains you agreed to in the domain selection form. In this stage of the evaluation you will score each question on the two criteria below, using a 5-point scale, resulting in two scores per question:

- *Ease of Use*: How easy is it for the SaaS provider to gather the information required to answer the question? (1 - Very difficult, 5 - Very easy)
- *Usefulness*: How useful are the insights extracted by the question for awarding a certification mark? (1 – Very useless, 5 - Very useful)

Framework evaluation - Stage 2

At this point your selected parts of the SaaS Continuity Guarantee framework have been reviewed. Now we will start the open-ended question stage of the framework evaluation. This stage is geared toward evaluating the framework as a whole.

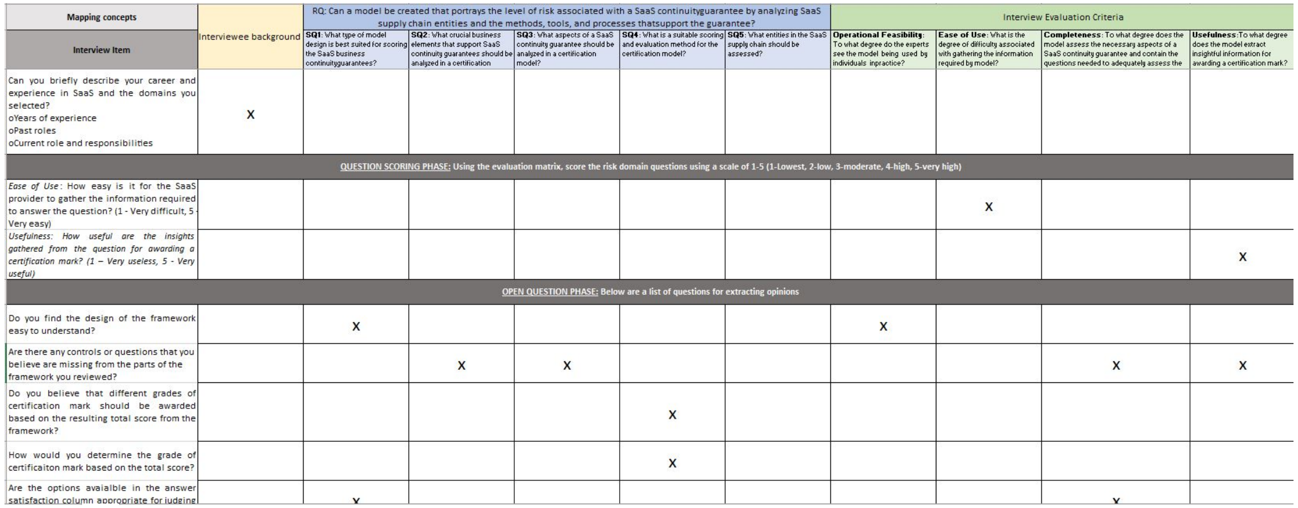
- Do you find the design of the framework easy to understand?
- Are there any controls or questions that you believe are missing from the part of the framework you review?
- Do you believe that different grades of certification mark should be awarded based on the resulting total score from the framework? How would you determine what grade is awarded based on the total score?
- Are the options avaialble in the answer satisfaction column appropriate for judging the question answers?
- Is there anything else you would like to see included in the framework?

Closing questions

- Do you think that only the SaaS provider should be assessed and why?
- Do you see yourself or a collegue making using of this framework in the future?
- Do you have any further comments towards the framework?

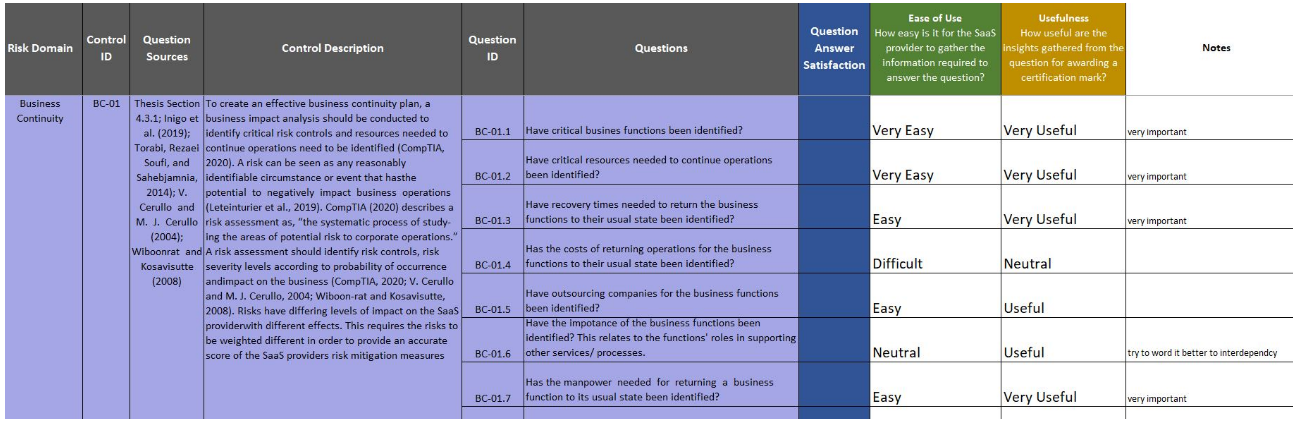
End of Interview

B.4 Interview Question Mapping Matrix Snippet



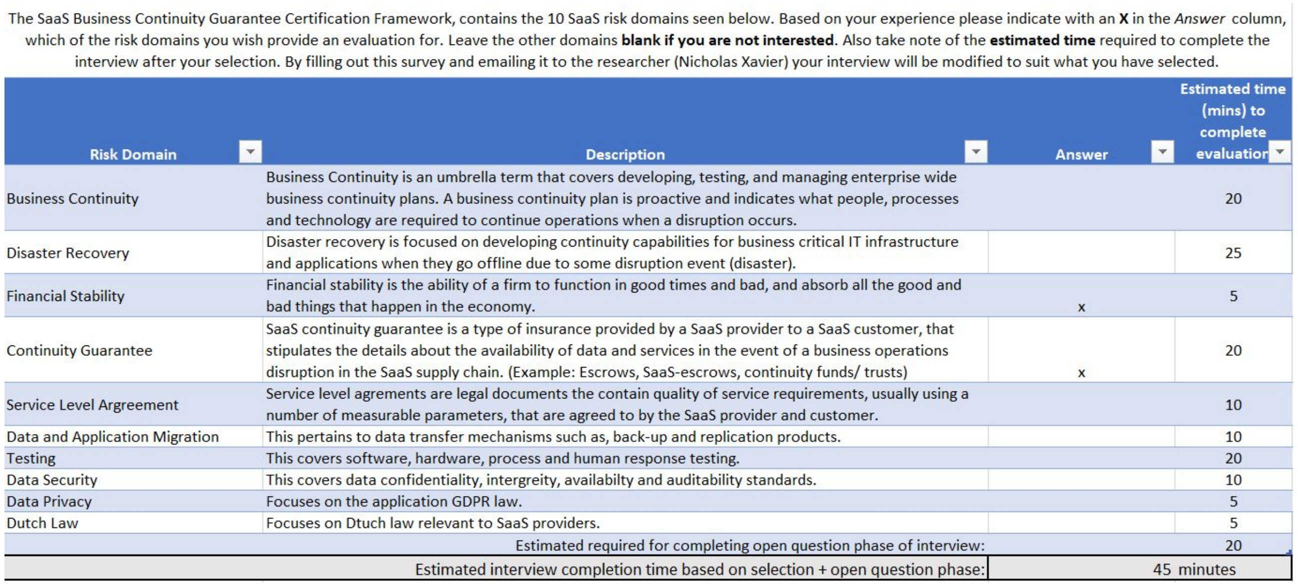
Mapping concepts	Interviewee background	RQ: Can a model be created that portrays the level of risk associated with a SaaS continuityguarantee by analyzing SaaS supply chain entities and the methods, tools, and processes thatsupport the guarantee?					Interview Evaluation Criteria			
Interview Item		**SQ1**: What type of model design is best suited for scoring the SaaS business continuityguarantees?	**SQ2**: What crucial business elements that support SaaS continuity guarantees should be analyzed in a certification	**SQ3**: What aspects of a SaaS continuity guarantee should be analyzed in a certification model?	**SQ4**: What is a suitable scoring and evaluation method for the certification model?	**SQ5**: What entities in the SaaS supply chain should be assessed?	**Operational Feasibility**: To what degree do the experts see the model being used by individuals inpractice?	**Ease of Use**: What is the degree of difficulty associated with gathering the information required by model?	**Completeness**: To what degree does the model assess the necessary aspects of a SaaS continuity guarantee and contain the questions needed to adequately assess the	**Usefulness**:To what degree does the model extract insightful information for awarding a certification mark?
Can you briefly describe your career and experience in SaaS and the domains you selected? oYears of experience oPast roles oCurrent role and responsibilities	X									
QUESTION SCORING PHASE: Using the evaluation matrix, score the risk domain questions using a scale of 1-5 (1-Lowest, 2-low, 3-moderate, 4-high, 5-very high)										
Ease of Use: How easy is it for the SaaS provider to gather the information required to answer the question? (1 - Very difficult, 5 - Very easy)								X		
Usefulness: How useful are the insights gathered from the question for awarding a certification mark? (1 – Very useless, 5 - Very useful)										X
OPEN QUESTION PHASE: Below are a list of questions for extracting opinions										
Do you find the design of the framework easy to understand?		X					X			
Are there any controls or questions that you believe are missing from the parts of the framework you reviewed?			X	X					X	X
Do you believe that different grades of certification mark should be awarded based on the resulting total score from the framework?					X					
How would you determine the grade of certificaiton mark based on the total score?					X					
Are the options avaialble in the answer satisfaction column appropriate for judging		X							X	

B.5 Framework Evaluation Form Snippet



Risk Domain	Control ID	Question Sources	Control Description	Question ID	Questions	Question Answer Satisfaction	Ease of Use How easy is it for the SaaS provider to gather the information required to answer the question?	Usefulness How useful are the insights gathered from the question for awarding a certification mark?	Notes
Business Continuity	BC-01	Thesis Section 4.3.1; Inigo et al. (2019); Torabi, Rezaei Soufi, and Sahebjamnia, 2014); V. Cerullo and M. J. Cerullo (2004); Wiboonrat and Kosavisutte (2008)	To create an effective business continuity plan, a business impact analysis should be conducted to identify critical risk controls and resources needed to continue operations need to be identified (CompTIA, 2020). A risk can be seen as any reasonably identifiable circumstance or event that hasthe potential to negatively impact business operations (Leteinturier et al., 2019). CompTIA (2020) describes a risk assessment as, “the systematic process of studying the areas of potential risk to corporate operations.” A risk assessment should identify risk controls, risk severity levels according to probability of occurrence andimpact on the business (CompTIA, 2020; V. Cerullo and M. J. Cerullo, 2004; Wiboon-rat and Kosavisutte, 2008). Risks have differing levels of impact on the SaaS providerwith different effects. This requires the risks to be weighted different in order to provide an accurate score of the SaaS providers risk mitigation measures	BC-01.1	Have critical busines functions been identified?		Very Easy	Very Useful	very important
				BC-01.2	Have critical resources needed to continue operations been identified?		Very Easy	Very Useful	very important
				BC-01.3	Have recovery times needed to return the business functions to their usual state been identified?		Easy	Very Useful	very important
				BC-01.4	Has the costs of returning operations for the business functions to their usual state been identified?		Difficult	Neutral	
				BC-01.5	Have outsourcing companies for the business functions been identified?		Easy	Useful	
				BC-01.6	Have the impotance of the business functions been identified? This relates to the functions' roles in supporting other services/ processes.		Neutral	Useful	try to word it better to interdependcy
				BC-01.7	Has the manpower needed for returning a business function to its usual state been identified?		Easy	Very Useful	very important

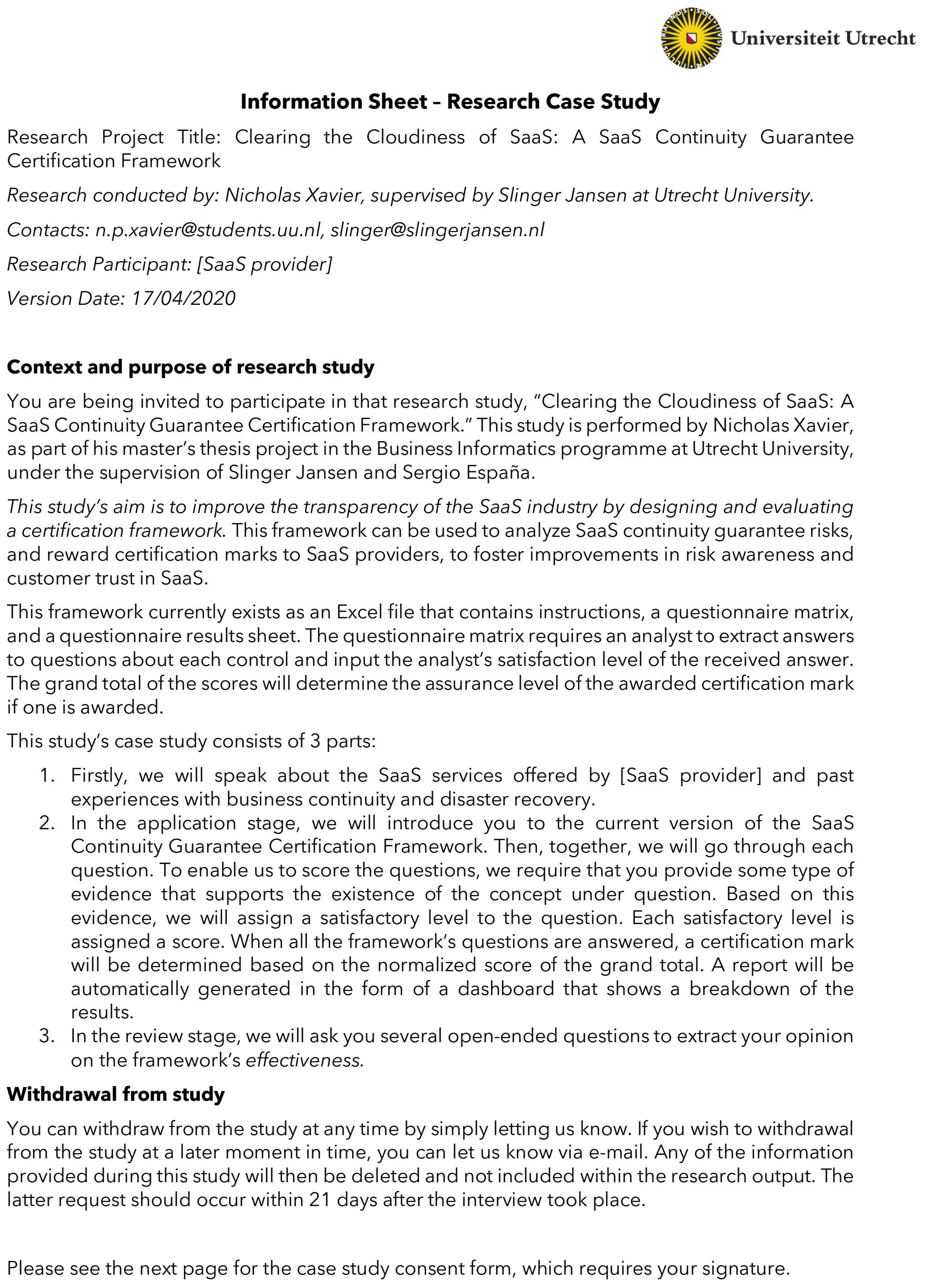
B.6 Expert Domain Selection Form



The SaaS Business Continuity Guarantee Certification Framework, contains the 10 SaaS risk domains seen below. Based on your experience please indicate with an **X** in the *Answer* column, which of the risk domains you wish provide an evaluation for. Leave the other domains **blank if you are not interested**. Also take note of the **estimated time** required to complete the interview after your selection. By filling out this survey and emailing it to the researcher (Nicholas Xavier) your interview will be modified to suit what you have selected.

Risk Domain	Description	Answer	Estimated time (mins) to complete evaluation
Business Continuity	Business Continuity is an umbrella term that covers developing, testing, and managing enterprise wide business continuity plans. A business continuity plan is proactive and indicates what people, processes and technology are required to continue operations when a disruption occurs.		20
Disaster Recovery	Disaster recovery is focused on developing continuity capabilities for business critical IT infrastructure and applications when they go offline due to some disruption event (disaster).		25
Financial Stability	Financial stability is the ability of a firm to function in good times and bad, and absorb all the good and bad things that happen in the economy.	x	5
Continuity Guarantee	SaaS continuity guarantee is a type of insurance provided by a SaaS provider to a SaaS customer, that stipulates the details about the availability of data and services in the event of a business operations disruption in the SaaS supply chain. (Example: Escrows, SaaS-escrows, continuity funds/ trusts)	x	20
Service Level Argreement	Service level agrements are legal documents the contain quality of service requirements, usually using a number of measurable parameters, that are agreed to by the SaaS provider and customer.		10
Data and Application Migration	This pertains to data transfer mechanisms such as, back-up and replication products.		10
Testing	This covers software, hardware, process and human response testing.		20
Data Security	This covers data confidentiality, intergreity, availabilty and auditability standards.		10
Data Privacy	Focuses on the application GDPR law.		5
Dutch Law	Focuses on Dtuch law relevant to SaaS providers.		5
	Estimated required for completing open question phase of interview:		20
	Estimated interview completion time based on selection + open question phase:	45 minutes	

B.7 Case Study Research Information Sheet



Universiteit Utrecht

Information Sheet – Research Case Study

Research Project Title: Clearing the Cloudiness of SaaS: A SaaS Continuity Guarantee Certification Framework

Research conducted by: Nicholas Xavier, supervised by Slinger Jansen at Utrecht University.

Contacts: n.p.xavier@students.uu.nl, slinger@slingerjansen.nl

Research Participant: [SaaS provider]

Version Date: 17/04/2020

Context and purpose of research study

You are being invited to participate in that research study, "Clearing the Cloudiness of SaaS: A SaaS Continuity Guarantee Certification Framework." This study is performed by Nicholas Xavier, as part of his master's thesis project in the Business Informatics programme at Utrecht University, under the supervision of Slinger Jansen and Sergio España.

This study's aim is to improve the transparency of the SaaS industry by designing and evaluating a certification framework. This framework can be used to analyze SaaS continuity guarantee risks, and reward certification marks to SaaS providers, to foster improvements in risk awareness and customer trust in SaaS.

This framework currently exists as an Excel file that contains instructions, a questionnaire matrix, and a questionnaire results sheet. The questionnaire matrix requires an analyst to extract answers to questions about each control and input the analyst's satisfaction level of the received answer. The grand total of the scores will determine the assurance level of the awarded certification mark if one is awarded.

This study's case study consists of 3 parts:

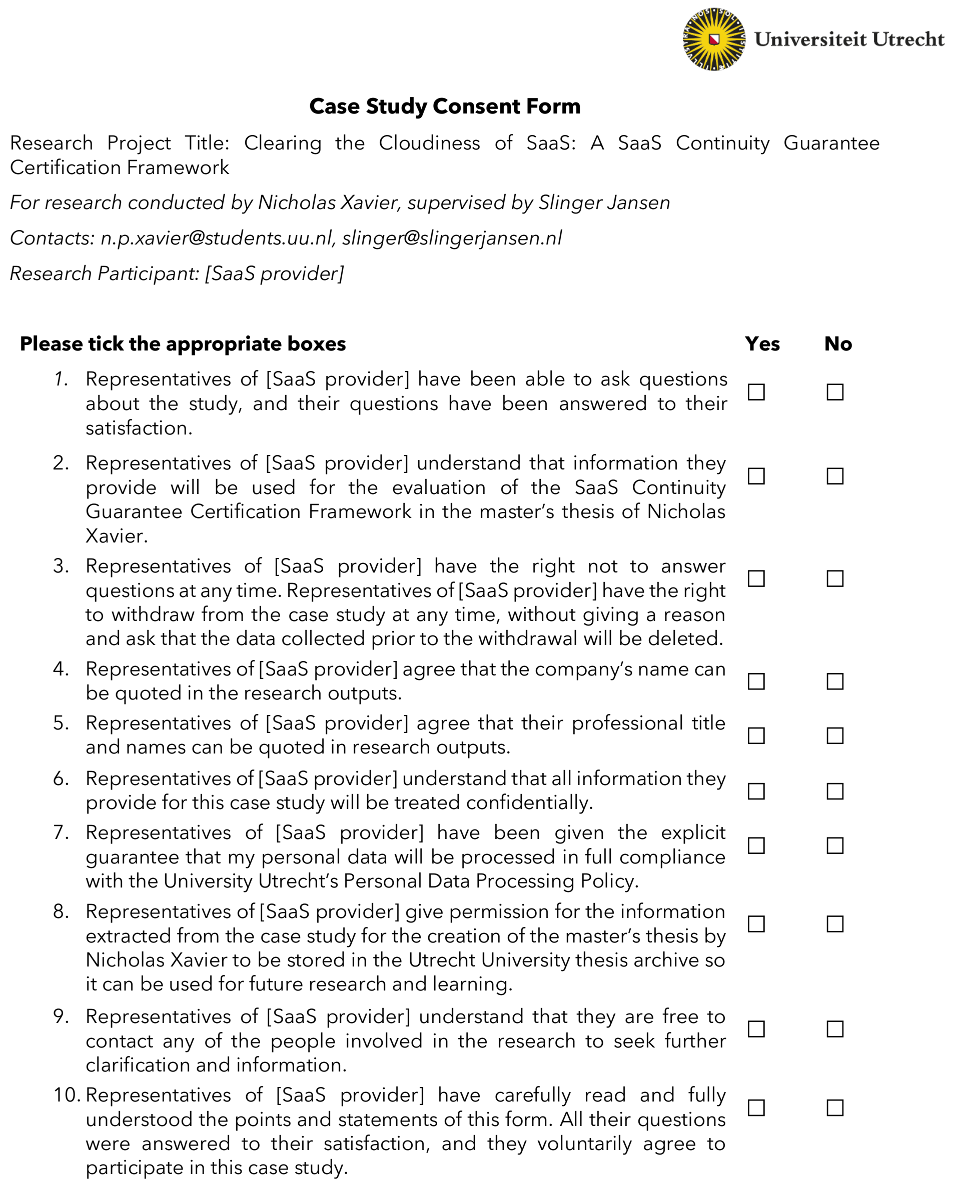
1. Firstly, we will speak about the SaaS services offered by [SaaS provider] and past experiences with business continuity and disaster recovery.
2. In the application stage, we will introduce you to the current version of the SaaS Continuity Guarantee Certification Framework. Then, together, we will go through each question. To enable us to score the questions, we require that you provide some type of evidence that supports the existence of the concept under question. Based on this evidence, we will assign a satisfactory level to the question. Each satisfactory level is assigned a score. When all the framework's questions are answered, a certification mark will be determined based on the normalized score of the grand total. A report will be automatically generated in the form of a dashboard that shows a breakdown of the results.
3. In the review stage, we will ask you several open-ended questions to extract your opinion on the framework's *effectiveness*.

Withdrawal from study

You can withdraw from the study at any time by simply letting us know. If you wish to withdrawal from the study at a later moment in time, you can let us know via e-mail. Any of the information provided during this study will then be deleted and not included within the research output. The latter request should occur within 21 days after the interview took place.

Please see the next page for the case study consent form, which requires your signature.

B.8 Case Study Consent Form and Guide



Universiteit Utrecht

Case Study Consent Form

Research Project Title: Clearing the Cloudiness of SaaS: A SaaS Continuity Guarantee Certification Framework

For research conducted by Nicholas Xavier, supervised by Slinger Jansen

Contacts: n.p.xavier@students.uu.nl, slinger@slingerjansen.nl

Research Participant: [SaaS provider]

Please tick the appropriate boxes	**Yes**	**No**
1. Representatives of [SaaS provider] have been able to ask questions about the study, and their questions have been answered to their satisfaction.	□	□
2. Representatives of [SaaS provider] understand that information they provide will be used for the evaluation of the SaaS Continuity Guarantee Certification Framework in the master's thesis of Nicholas Xavier.	□	□
3. Representatives of [SaaS provider] have the right not to answer questions at any time. Representatives of [SaaS provider] have the right to withdraw from the case study at any time, without giving a reason and ask that the data collected prior to the withdrawal will be deleted.	□	□
4. Representatives of [SaaS provider] agree that the company's name can be quoted in the research outputs.	□	□
5. Representatives of [SaaS provider] agree that their professional title and names can be quoted in research outputs.	□	□
6. Representatives of [SaaS provider] understand that all information they provide for this case study will be treated confidentially.	□	□
7. Representatives of [SaaS provider] have been given the explicit guarantee that my personal data will be processed in full compliance with the University Utrecht's Personal Data Processing Policy.	□	□
8. Representatives of [SaaS provider] give permission for the information extracted from the case study for the creation of the master's thesis by Nicholas Xavier to be stored in the Utrecht University thesis archive so it can be used for future research and learning.	□	□
9. Representatives of [SaaS provider] understand that they are free to contact any of the people involved in the research to seek further clarification and information.	□	□
10. Representatives of [SaaS provider] have carefully read and fully understood the points and statements of this form. All their questions were answered to their satisfaction, and they voluntarily agree to participate in this case study.	□	□

11. Representatives of [SaaS provider] obtained a copy of this consent form co-signed by the interviewer. □ □

________________________ ____________________
[SaaS provider] Representative Signature Date

________________________ ____________________
Researcher Signature Date

Universiteit Utrecht

Case Study Guide

Introduction

The case study's time frame is dependant on the speed at which [SaaS provider] can provide the evidence required to score the questions presented in the framework. This evidence will be assessed by the research team, and an appropriate satisfaction level is given.

General information

- Can you briefly describe [SaaS provider] and its experience SaaS?
  Prompts:
  - Number of employees
  - Years in operation
  - Description of SaaS services
  - Past experience with business continuity plan/ disaster recovery plan initiation

Framework application

The steps involved in this stage are described in the bullet points below:

- For this stage of the case study, questions from the framework will be presented to [SaaS provider].
- For each question, [SaaS provider] will provide appropriate evidence to the research team for assessment.
- The research team will assess the evidence and assign a satisfaction level to the relevant question.
- The above steps will be repeated until all the questions in the framework are answered.
- Upon completion, a short report of the results will be given to [SaaS provider] for review.

Framework effectiveness review

In this study, effectiveness is defined as, "To what degree do insights gathered [from the framework] portray the level of risk associated with a SaaS continuity guarantee?" To validate the framework's effectiveness, [SaaS provider] is asked to answer the open-ended bulleted questions below. The questions are meant to initiate a reflection on the degree to which the insights gathered from the questions portray the level of risk associated with a SaaS continuity guarantee. The statements have been sourced from published certification scheme requirements for information communication technology (ICT) security frameworks by the *European Union Agency for Cybersecurity*.

- Does the framework assess controls that protect stored, transmitted, or otherwise processed data against accidental or unauthorized destruction, loss or alteration, or lack of availability during the entire life cycle of the ICT product, ICT service, or ICT process?
- Does the framework assess controls that ensure authorized persons, programs, or machines are able only to access the data, services, or functions to which their access rights refer; to identify and document known dependencies and vulnerabilities?
- Does the framework assess controls that record which data, services, or functions have been accessed, used, or otherwise processed, at what times and by whom?
- Does the framework assess controls that make it possible to check which data, services, or functions have been accessed, used, or otherwise processed, at what times and by whom?
- Does the framework assess controls that verify that ICT products, ICT services, and ICT processes do not contain known vulnerabilities?
- Does the framework assess controls that restore the availability and access to data, services, and functions in a timely manner in the event of a physical or technical disruption event?
- Does the framework assess controls that ensure that ICT products, ICT services, and ICT processes are secure by default and by design that ICT products, ICT services, and ICT processes are provided with up-to-date software and hardware that do not contain publicly known vulnerabilities, and are provided with mechanisms for secure updates?

End

Appendix C

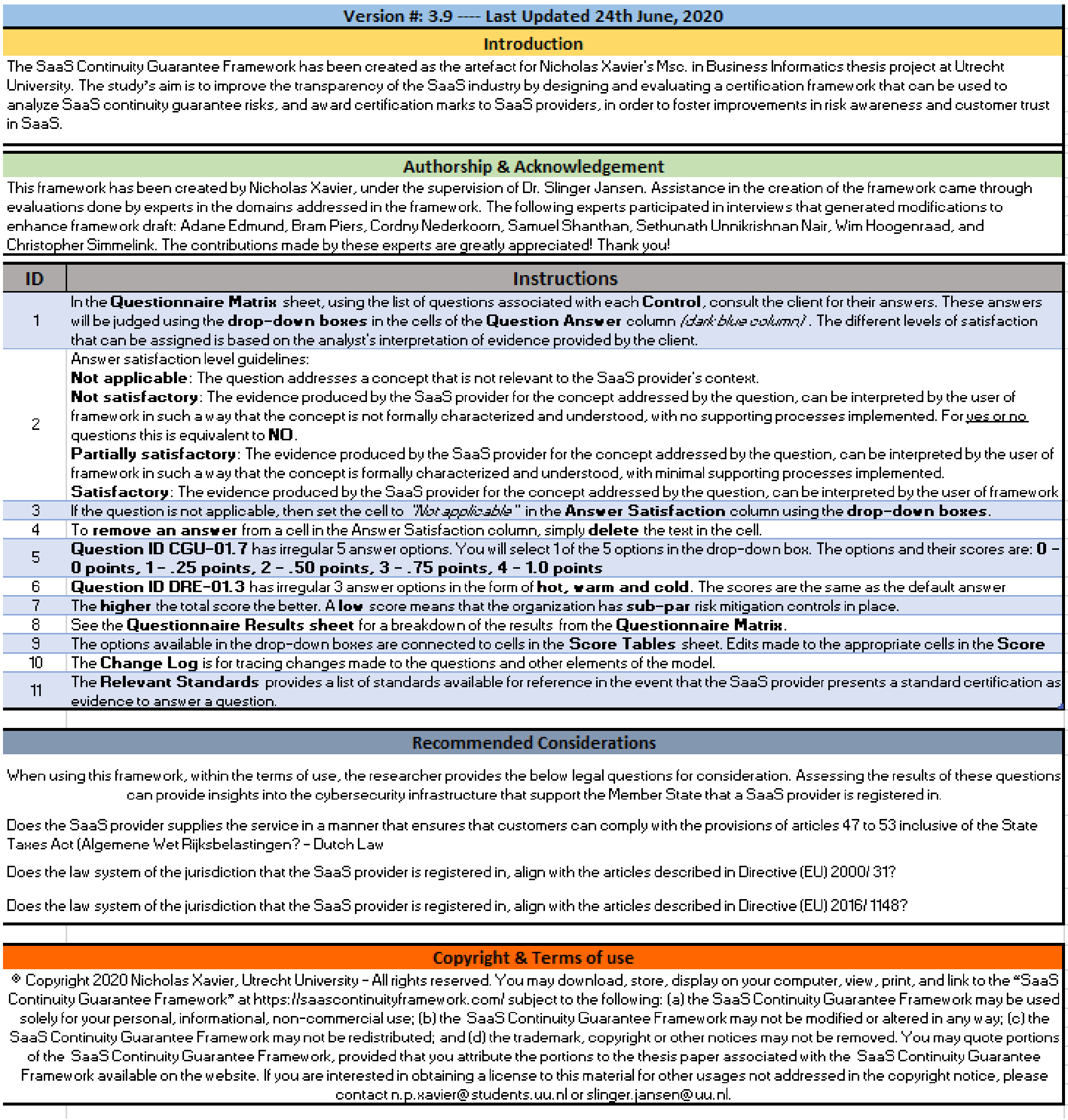
Framework Draft Snippets

C.1 Relevant standards table from CloudWatch2 (2017), Elliott, Thomas, and Muhammad (2020), and Kosutic (2015). Seen in framework as a sheet entitled, *Standards*.

Group	Standard	Publisher
Portability	Open Virtualization Format (OVF)	Distributed Management Task Force (DMTF)
	Topology and Orchestration Services for Applications (TOSCA)	Organization for the Advancement of Structured Information Standards (OASIS)
Interoperability	Open Cloud Computing Interface (OCCI) - **IaaS layer**	Open Grid Forum
	Cloud Infrastructure Management Interface (CIMI) - **IaaS layer**	Distributed Management Task Force (DMTF)
	Cloud Data Management Interface (CDMI) - **PaaS layer**	The Storage Networking Industry Association (SNIA)
	Cloud Application Management Protocol (CAMP) - **PaaS layer**	Organization for the Advancement of Structured Information Standards (OASIS)
	ISO/IEC JTC 1/SC family of standards	International Standards Organization (ISO)
	IP (v4, v6), TCP, HTTP, SSL/TLS, HTML, XML, REST, Atom, AtomPub, RSS, and JavaScript/JSON, OpenID, Odata, CDMI, AMQP, and XMPP, XML - **SaaS layer**	Variety of publishers
Security (including BC standards)	ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27004, ISO/IEC 27005, ISO/IEC TR 27008:2011, ISO/IEC 24762:2008, ISO/IEC 27031:2011, ISO/IEC 27035, ISO 31000:2009, ISO/IEC 38500:2008, ISO 22301, ISO 9001, ISO 14001, ISO 45001, ISO/IEC 20000-1, ISO/IEC JTC 1/SC family of standards	International Standards Organization (ISO)
	BS 7858:2006+A2:2009, BS 25999-1, PD 25111:2010, PD 25666:2010, PAS 200:2011, BS 11200, BS 10012:2017	British Standards (BSI)
	NIST 800-53 Rev.4 Security Controls, NIST Security Reference Architecture, NIST SP 800-55, NIST SP 800-61	National Institute of Standards and Technology (NIST)
	Cloud Controls Matrix, Open Certification Framework, Cloud Trust Protocol, Cloud Audit, Privacy Level Agreement	Cloud Security Alliance (CSA)
	EuroCloud Star Audit (ESCA)	EuroCloud
	Data Security Framework	Open Data Center Alliance

Control Objectives for Information and related Technology (COBIT)	Information Systems Audit and Control Association (ISACA)
ITIL v.3 (international)	Information Technology Infrastructure Library
NFPA 1600	National Fire Protection Agency
Zeker-Online Framework of Standards	Zeker-Online
SOC 1, SOC 2	Service Organization Control (SOC)

C.2 User Guide



Version #: 3.9 ---- Last Updated 24th June, 2020

Introduction

The SaaS Continuity Guarantee Framework has been created as the artefact for Nicholas Xavier's Msc. in Business Informatics thesis project at Utrecht University. The study's aim is to improve the transparency of the SaaS industry by designing and evaluating a certification framework that can be used to analyze SaaS continuity guarantee risks, and award certification marks to SaaS providers, in order to foster improvements in risk awareness and customer trust in SaaS.

Authorship & Acknowledgement

This framework has been created by Nicholas Xavier, under the supervision of Dr. Slinger Jansen. Assistance in the creation of the framework came through evaluations done by experts in the domains addressed in the framework. The following experts participated in interviews that generated modifications to enhance framework draft: Adane Edmund, Bram Piers, Cordny Nederkoorn, Samuel Shanthan, Sethunath Unnikrishnan Nair, Wim Hoogenraad, and Christopher Simmelink. The contributions made by these experts are greatly appreciated! Thank you!

ID	Instructions
1	In the **Questionnaire Matrix** sheet, using the list of questions associated with each **Control**, consult the client for their answers. These answers will be judged using the **drop-down boxes** in the cells of the **Question Answer** column *(dark blue column)*. The different levels of satisfaction that can be assigned is based on the analyst's interpretation of evidence provided by the client.
2	Answer satisfaction level guidelines: **Not applicable**: The question addresses a concept that is not relevant to the SaaS provider's context. **Not satisfactory**: The evidence produced by the SaaS provider for the concept addressed by the question, can be interpreted by the user of framework in such a way that the concept is not formally characterized and understood, with no supporting processes implemented. For yes or no questions this is equivalent to **NO**. **Partially satisfactory**: The evidence produced by the SaaS provider for the concept addressed by the question, can be interpreted by the user of framework in such a way that the concept is formally characterized and understood, with minimal supporting processes implemented. **Satisfactory**: The evidence produced by the SaaS provider for the concept addressed by the question, can be interpreted by the user of framework
3	If the question is not applicable, then set the cell to *"Not applicable"* in the **Answer Satisfaction** column using the **drop-down boxes**.
4	To **remove an answer** from a cell in the Answer Satisfaction column, simply **delete** the text in the cell.
5	**Question ID CGU-01.7** has irregular 5 answer options. You will select 1 of the 5 options in the drop-down box. The options and their scores are: **0 - 0 points, 1 - .25 points, 2 - .50 points, 3 - .75 points, 4 - 1.0 points**
6	**Question ID DRE-01.3** has irregular 3 answer options in the form of **hot, warm and cold**. The scores are the same as the default answer
7	The **higher** the total score the better. A **low** score means that the organization has **sub-par** risk mitigation controls in place.
8	See the **Questionnaire Results sheet** for a breakdown of the results from the **Questionnaire Matrix**.
9	The options available in the drop-down boxes are connected to cells in the **Score Tables** sheet. Edits made to the appropriate cells in the **Score**
10	The **Change Log** is for tracing changes made to the questions and other elements of the model.
11	The **Relevant Standards** provides a list of standards available for reference in the event that the SaaS provider presents a standard certification as evidence to answer a question.

Recommended Considerations

When using this framework, within the terms of use, the researcher provides the below legal questions for consideration. Assessing the results of these questions can provide insights into the cybersecurity infrastructure that support the Member State that a SaaS provider is registered in.

Does the SaaS provider supplies the service in a manner that ensures that customers can comply with the provisions of articles 47 to 53 inclusive of the State Taxes Act (Algemene Wet Rijksbelastingen? - Dutch Law

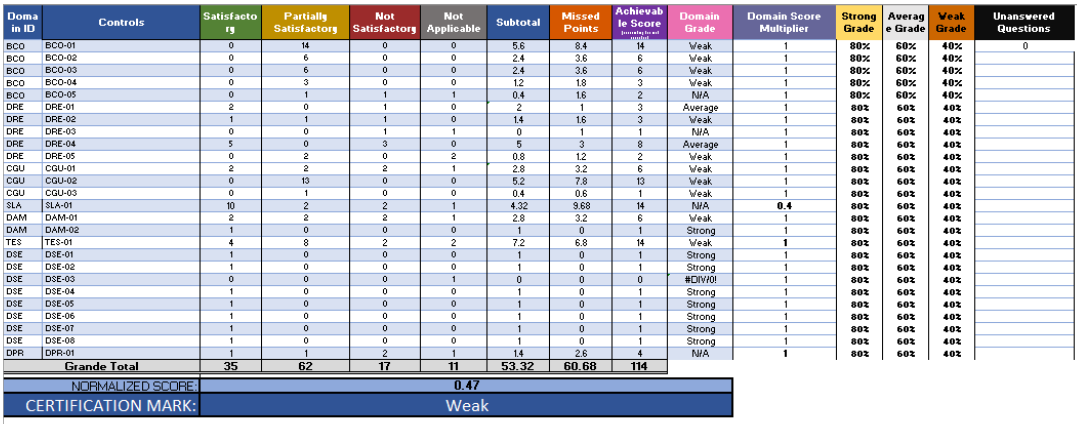
Does the law system of the jurisdiction that the SaaS provider is registered in, align with the articles described in Directive (EU) 2000/ 31?

Does the law system of the jurisdiction that the SaaS provider is registered in, align with the articles described in Directive (EU) 2016/ 1148?

Copyright & Terms of use

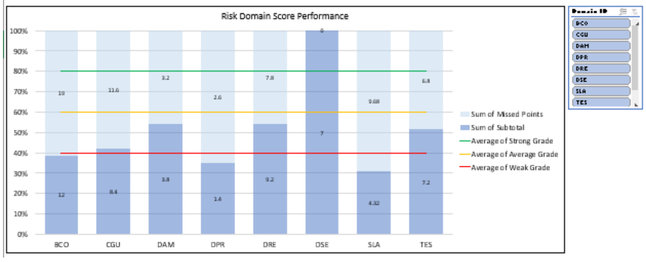
® Copyright 2020 Nicholas Xavier, Utrecht University - All rights reserved. You may download, store, display on your computer, view, print, and link to the "SaaS Continuity Guarantee Framework" at https://saascontinuityframework.com/ subject to the following: (a) the SaaS Continuity Guarantee Framework may be used solely for your personal, informational, non-commercial use; (b) the SaaS Continuity Guarantee Framework may not be modified or altered in any way; (c) the SaaS Continuity Guarantee Framework may not be redistributed; and (d) the trademark, copyright or other notices may not be removed. You may quote portions of the SaaS Continuity Guarantee Framework, provided that you attribute the portions to the thesis paper associated with the SaaS Continuity Guarantee Framework available on the website. If you are interested in obtaining a license to this material for other usages not addressed in the copyright notice, please contact n.p.xavier@students.uu.nl or slinger.jansen@uu.nl.

C.3 Questionnaire Report

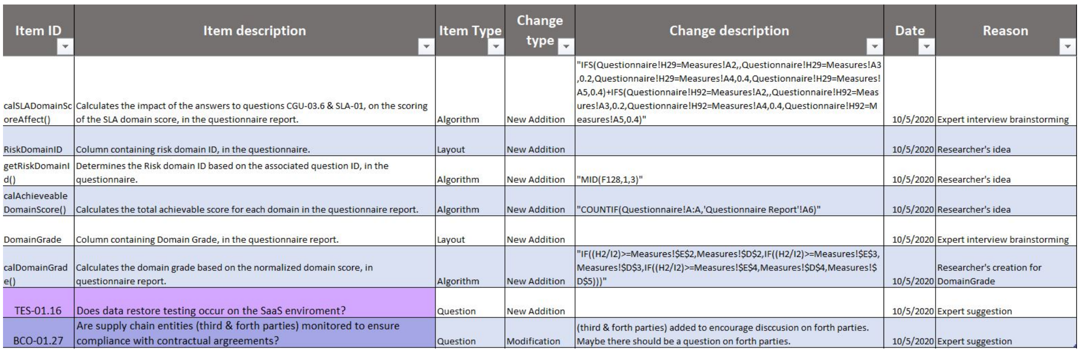


Domain ID	Controls	Satisfactory	Partially Satisfactory	Not Satisfactory	Not Applicable	Subtotal	Missed Points	Achievable Score	Domain Grade	Domain Score Multiplier	Strong Grade	Average Grade	Weak Grade	Unanswered Questions
BCO	BCO-01	0	14	0	0	5.6	8.4	14	Weak	1	80%	60%	40%	0
BCO	BCO-02	0	6	0	0	2.4	3.6	6	Weak	1	80%	60%	40%	
BCO	BCO-03	0	6	0	0	2.4	3.6	6	Weak	1	80%	60%	40%	
BCO	BCO-04	0	3	0	0	1.2	1.8	3	Weak	1	80%	60%	40%	
BCO	BCO-05	0	1	1	1	0.4	1.6	2	N/A	1	80%	60%	40%	
DRE	DRE-01	2	0	1	0	2	1	3	Average	1	80%	60%	40%	
DRE	DRE-02	1	1	1	0	1.4	1.6	3	Weak	1	80%	60%	40%	
DRE	DRE-03	0	0	1	1	0	1	1	N/A	1	80%	60%	40%	
DRE	DRE-04	5	0	3	0	5	3	8	Average	1	80%	60%	40%	
DRE	DRE-05	0	2	0	2	0.8	1.2	2	Weak	1	80%	60%	40%	
CGU	CGU-01	2	2	2	1	2.8	3.2	6	Weak	1	80%	60%	40%	
CGU	CGU-02	0	13	0	0	5.2	7.8	13	Weak	1	80%	60%	40%	
CGU	CGU-03	0	1	0	0	0.4	0.6	1	Weak	1	80%	60%	40%	
SLA	SLA-01	10	2	2	1	4.32	9.68	14	N/A	0.4	80%	60%	40%	
DAM	DAM-01	2	2	2	1	2.8	3.2	6	Weak	1	80%	60%	40%	
DAM	DAM-02	1	0	0	0	1	0	1	Strong	1	80%	60%	40%	
TES	TES-01	4	8	2	2	7.2	6.8	14	Weak	1	80%	60%	40%	
DSE	DSE-01	1	0	0	0	1	0	1	Strong	1	80%	60%	40%	
DSE	DSE-02	1	0	0	0	1	0	1	Strong	1	80%	60%	40%	
DSE	DSE-03	0	0	0	1	0	0	0	#DIV/0!	1	80%	60%	40%	
DSE	DSE-04	1	0	0	0	1	0	1	Strong	1	80%	60%	40%	
DSE	DSE-05	1	0	0	0	1	0	1	Strong	1	80%	60%	40%	
DSE	DSE-06	1	0	0	0	1	0	1	Strong	1	80%	60%	40%	
DSE	DSE-07	1	0	0	0	1	0	1	Strong	1	80%	60%	40%	
DSE	DSE-08	1	0	0	0	1	0	1	Strong	1	80%	60%	40%	
DPR	DPR-01	1	1	2	1	1.4	2.6	4	N/A	1	80%	60%	40%	
Grande Total		**35**	**62**	**17**	**11**	**53.32**	**60.68**	**114**						

NORMALIZED SCORE:	**0.47**
CERTIFICATION MARK:	Weak



C.4 Change Log

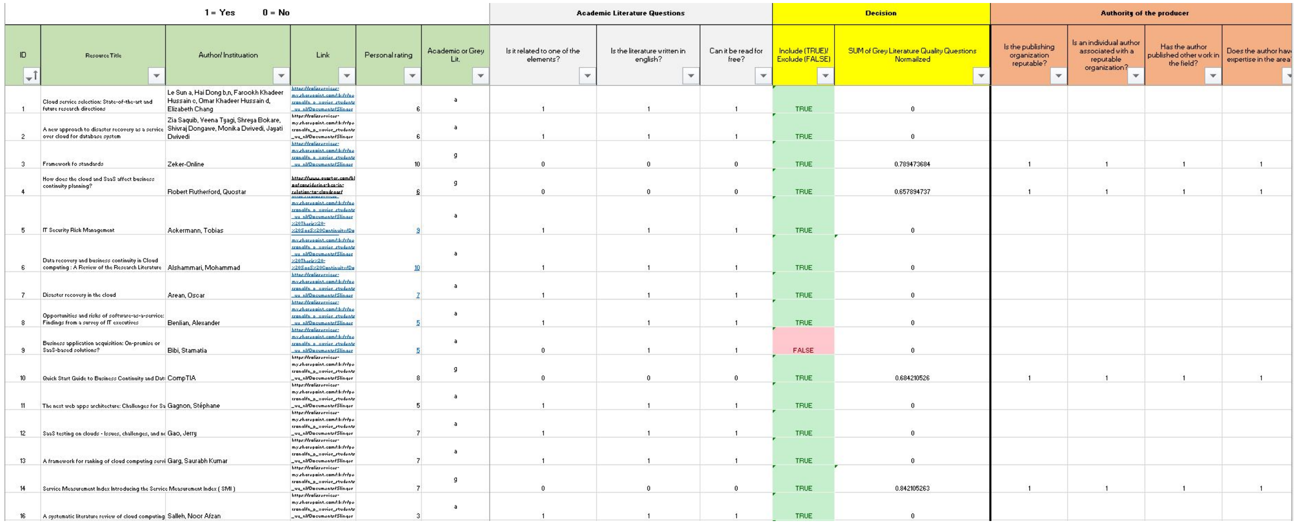


Item ID	Item description	Item Type	Change type	Change description	Date	Reason
calSLADomainScoreAffect()	Calculates the impact of the answers to questions CGU-03.6 & SLA-01, on the scoring of the SLA domain score, in the questionnaire report.	Algorithm	New Addition	"IFS(Questionnaire!H29=Measures!A2,,Questionnaire!H29=Measures!A3,0.2,Questionnaire!H29=Measures!A4,0.4,Questionnaire!H29=Measures!A5,0.4)+IFS(Questionnaire!H92=Measures!A2,,Questionnaire!H92=Measures!A3,0.2,Questionnaire!H92=Measures!A4,0.4,Questionnaire!H92=Measures!A5,0.4)"	10/5/2020	Expert interview brainstorming
RiskDomainID	Column containing risk domain ID, in the questionnaire.	Layout	New Addition		10/5/2020	Researcher's idea
getRiskDomainId()	Determines the Risk domain ID based on the associated question ID, in the questionnaire.	Algorithm	New Addition	"MID(F128,1,3)"	10/5/2020	Researcher's idea
calAchieveable DomainScore()	Calculates the total achievable score for each domain in the questionnaire report.	Algorithm	New Addition	"COUNTIF(Questionnaire!A:A,'Questionnaire Report'!A6)"	10/5/2020	Researcher's idea
DomainGrade	Column containing Domain Grade, in the questionnaire report.	Layout	New Addition		10/5/2020	Expert interview brainstorming
calDomainGrade()	Calculates the domain grade based on the normalized domain score, in questionnaire report.	Algorithm	New Addition	"IF((H2/I2)>=Measures!$E$2,Measures!$D$2,IF((H2/I2)>=Measures!$E$3,Measures!$D$3,IF((H2/I2)>=Measures!$E$4,Measures!$D$4,Measures!$D$5)))"	10/5/2020	Researcher's creation for DomainGrade
TES-01.16	Does data restore testing occur on the SaaS enviroment?	Question	New Addition		10/5/2020	Expert suggestion
BCO-01.27	Are supply chain entities (third & forth parties) monitored to ensure compliance with contractual argreements?	Question	Modification	(third & forth parties) added to encourage disccusion on forth parties. Maybe there should be a question on forth parties.	10/5/2020	Expert suggestion

Appendix D

Supplement

D.1 Data Collection Form Snippet



1 = Yes 0 = No						Academic Literature Questions			Decision		Authority of the producer			
ID	Resource Title	Author/ Instituation	Link	Personal rating	Academic or Grey Lit.	Is it related to one of the elements?	Is the literature written in english?	Can it be read for free?	Include (TRUE)/ Exclude (FALSE)	SUM of Grey Literature Quality Questions Normailzed	Is the publishing organization reputable?	Is an individual author associated with a reputable organization?	Has the author published other work in the field?	Does the author hav expertise in the area
1	Cloud service selection: State-of-the-art and future research directions	Le Sun a, Hai Dong b,n, Farookh Khadeer Hussain c, Omar Khadeer Hussain d, Elizabeth Chang	https://ralizservices- my.sharepoint.com/:b:/r/pe rsonal/n_p_xavier_students _uu_nl/Documents/Slinger	6	a	1	1	1	TRUE	0				
2	A new approach to disaster recovery as a service over cloud for database system	Zia Saquib, Veena Tyagi, Shreya Bokare, Shivraj Dongawe, Monika Dwivedi, Jayati Dwivedi	https://ralizservices- my.sharepoint.com/:b:/r/pe rsonal/n_p_xavier_students _uu_nl/Documents/Slinger	6	a	1	1	1	TRUE	0				
3	Framework fo standards	Zeker-Online	https://ralizservices- my.sharepoint.com/:b:/r/pe rsonal/n_p_xavier_students _uu_nl/Documents/Slinger	10	g	0	0	0	TRUE	0.789473684	1	1	1	1
4	How does the cloud and SaaS affect business continuity planning?	Robert Rutherford, Quostar	https://www.quostar.com/bl og/considering-bcp-in- relation-to-cloudsaas/	6	g	0	0	0	TRUE	0.657894737	1	1	1	1
5	IT Security Risk Management	Ackermann, Tobias	my.sharepoint.com/:b:/r/pe rsonal/n_p_xavier_students _uu_nl/Documents/Slinger %20Thesis%20- %20SaaS%20Continuity/Do	9	a	1	1	1	TRUE	0				
6	Data recovery and business continuity in Cloud computing : A Review of the Research Literature	Alshammari, Mohammad	my.sharepoint.com/:b:/r/pe rsonal/n_p_xavier_students _uu_nl/Documents/Slinger %20Thesis%20- %20SaaS%20Continuity/Do	10	a	1	1	1	TRUE	0				
7	Disaster recovery in the cloud	Arean, Oscar	https://ralizservices- my.sharepoint.com/:b:/r/pe rsonal/n_p_xavier_students _uu_nl/Documents/Slinger	7	a	1	1	1	TRUE	0				
8	Opportunities and risks of software-as-a-service: Findings from a survey of IT executives	Benlian, Alexander	https://ralizservices- my.sharepoint.com/:b:/r/pe rsonal/n_p_xavier_students _uu_nl/Documents/Slinger	5	a	1	1	1	TRUE	0				
9	Business application acquisition: On-premise or SaaS-based solutions?	Bibi, Stamatia	https://ralizservices- my.sharepoint.com/:b:/r/pe rsonal/n_p_xavier_students _uu_nl/Documents/Slinger	5	a	0	1	1	FALSE	0				
10	Quick Start Guide to Business Continuity and Dat	CompTIA	https://ralizservices- my.sharepoint.com/:b:/r/pe rsonal/n_p_xavier_students _uu_nl/Documents/Slinger	8	g	0	0	0	TRUE	0.684210526	1	1	1	1
11	The next web apps architecture: Challenges for Sa	Gagnon, Stéphane	https://ralizservices- my.sharepoint.com/:b:/r/pe rsonal/n_p_xavier_students _uu_nl/Documents/Slinger	5	a	1	1	1	TRUE	0				
12	SaaS testing on clouds - Issues, challenges, and nc	Gao, Jerry	https://ralizservices- my.sharepoint.com/:b:/r/pe rsonal/n_p_xavier_students _uu_nl/Documents/Slinger	7	a	1	1	1	TRUE	0				
13	A framework for ranking of cloud computing servi	Garg, Saurabh Kumar	https://ralizservices- my.sharepoint.com/:b:/r/pe rsonal/n_p_xavier_students _uu_nl/Documents/Slinger	7	a	1	1	1	TRUE	0				
14	Service Measurement Index Introducing the Service Measurement Index (SMI)		https://ralizservices- my.sharepoint.com/:b:/r/pe rsonal/n_p_xavier_students _uu_nl/Documents/Slinger	7	g	0	0	0	TRUE	0.842105263	1	1	1	1
16	A systematic literature review of cloud computing	Salleh, Noor Afzan	https://ralizservices- my.sharepoint.com/:b:/r/pe rsonal/n_p_xavier_students _uu_nl/Documents/Slinger	3	a	1	1	1	TRUE	0				

Bibliography

Ackermann, Tobias (2012). *IT Security Risk Management*. 1st ed. Gabler Verlag. ISBN: 978-3-658-01114-7.

Adams, Mike et al. (2014). "An introduction to designing reliable cloud services". In: *Microsoft Corporation*, pp. 1–14.

Adams, Richard J., Palie Smart, and Anne Sigismund Huff (2017). "Shades of Grey: Guidelines for Working with the Grey Literature in Systematic Reviews for Management and Organizational Studies". In: *International Journal of Management Reviews* 19.4, pp. 432–454. ISSN: 14682370.

Al-Hujran, Omar et al. (2018). "Challenges of cloud computing adoption from the TOE framework perspective". In: *International Journal of e-Business Research* 14.3, pp. 77–94. ISSN: 1548114X.

Alali, Fatima A. and Chia Lun Yeh (2012). "Cloud computing: Overview and risk analysis". In: *Journal of Information Systems* 26.2, pp. 13–33. ISSN: 08887985.

Alhamad, Mohammed, Tharam Dillon, and Elizabeth Chang (2010). "Conceptual SLA framework for cloud computing". In: *4th IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST 2010)*, pp. 606–610.

Alhazmi, Omar H. and Yashwant K. Malaiya (2013). "Evaluating disaster recovery plans using the cloud". In: *Proceedings - Annual Reliability and Maintainability Symposium*. ISSN: 0149144X.

Alshammari, Mohammad, Ali Alwan, and Imad Alshaikhli (2016). "Data recovery and business continuity in Cloud computing : A Review of the Research Literature". In: *International Journal of Advancements in Computing Technology* 8, pp. 80–94.

Ambler, Scott W (2005). "The elements of UML (TM) 2.0 style". In:

Ampatzoglou, Apostolos et al. (2019). "Identifying, categorizing and mitigating threats to validity in software engineering secondary studies". In: *Information and Software Technology* 106.February 2018, pp. 201–230. ISSN: 09505849.

Anisetti, M. et al. (2016). "A certification framework for cloud-based services". In: *Proceedings of the ACM Symposium on Applied Computing*. ISBN: 9781450337397.

Arean, Oscar (2013). "Disaster recovery in the cloud". In: *Network Security* 9, pp. 5–7. ISSN: 13534858.

Armburst, Michael et al. (2010). "A view of cloud computing". In: *Communications of the ACM* 53.2, pp. 50–58. ISSN: 00225347.

Bannelier-Christakis, Karine and Theodore Christakis (2017). "Cyber-Attacks - Prevention - Reactions". In: Les Cahiers de la Revue Défense Nationale. (Visited on 06/09/2020).

Bibi, Stamatia, Dimitrios Katsaros, and Panayiotis Bozanis (2012). "Business application acquisition: On-premise or SaaS-based solutions?" In: *IEEE Software* 29.3, pp. 86–93. ISSN: 07407459.

Birke, Robert, Lydia Y. Chen, and Evgenia Smirni (2012). "Data centers in the cloud: A large scale performance study". In: *Proceedings - 2012 IEEE 5th International Conference on Cloud Computing, CLOUD 2012*, pp. 336–343.

Braun, Virginia and Victoria Clarke (2012). “Thematic analysis.” In: *APA handbook of research methods in psychology, Vol 2: Research designs: Quantitative, qualitative, neuropsychological, and biological.* 2, pp. 57–71.

Brinkkemper, Sjaak (1996). “Method engineering: engineering of information systems development methods and tools”. In: *Information and software technology* 38.4, pp. 275–280.

Bruin, Tonia de et al. (2005). “Understanding the main phases of developing a maturity assessment model”. In: *ACIS 2005 Proceedings - 16th Australasian Conference on Information Systems*. December.

Castillo-Montoya, Milagros (2016). “Preparing for interview research: The interview protocol refinement framework”. In: *Qualitative Report* 21.5, pp. 811–831. ISSN: 10520147.

Cerullo, Virginia and Michael J. Cerullo (2004). “Business continuity planning: A comprehensive approach”. In: *Information Systems Management* 21.3, pp. 70–78. ISSN: 10580530.

Chana, Inderveer and Sukhpal Singh (2014). “Quality of service and service level agreements for cloud environments: Issues and challenges”. In: *Cloud Computing*. Springer, pp. 51–72.

Cruzes, Daniela S and Tore Dybå (2010). “Synthesizing Evidence in Software Engineering Research”. In: *ESEM '10: Proceedings of the 2010 ACM-IEEE International Symposium on Empirical Software Engineering and Measurement*. 1, pp. 1–10.

Cruzes, Daniela S. and Tore Dybå (2011). “Recommended steps for thematic synthesis in software engineering”. In: *International Symposium on Empirical Software Engineering and Measurement*, pp. 275–284. ISSN: 19493770.

Dudouet, Florian, Andrew Edmonds, and Michael Erne (2015). “Reliable cloud-applications: An implementation through service orchestration”. In: *Proceedings: AIMC 2015 - Automated Incident Management in Cloud, 1st International Workshop, in conjunction with EuroSYS 2015*, pp. 1–6.

Dutta, A., G.C Peng, and A. Choudhary (2013). “Risks in Enterprise Cloud Computing: the Perspective of IT Experts”. In: *Journal of Computer Information Systems* 53.4, pp. 39–48.

Emerson, Robert Wall (2017). “Likert Scales”. In: *Journal of Visual Impairment & Blindness* 111.5, pp. 488–488. ISSN: 0145-482X.

Etikan, Ilker (2016). “Comparison of Convenience Sampling and Purposive Sampling”. In: *American Journal of Theoretical and Applied Statistics* 5.1, p. 1. ISSN: 2326-8999.

Fontaine, N and G d’Oliveira Martins (2000). “Directive 2000/31/EC of the European parliament and of the council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)”. In: *Official Journal of the European Communities*, pp. 1–13.

Freeman, Edward H. (2004). “Source code escrow”. In: *Information Systems Security* 13.1, pp. 8–11. ISSN: 1065898X.

Fuster, Gloria González and Lina Jasmontaite (2020). “Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights”. In: pp. 97–115.

Gao, Jerry, Xiaoying Bai, and Wei-Tek Tsai (2011). “Cloud testing-issues, challenges, needs and practice”. In: *Software Engineering: An International Journal* 1.1, pp. 9–23.

Gao, Jerry et al. (2013). "SaaS testing on clouds - Issues, challenges, and needs". In: *Proceedings - 2013 IEEE 7th International Symposium on Service-Oriented System Engineering, SOSE 2013* March, pp. 409–415.

Garousi, Vahid and Michael Felderer (2017). "Experience-based guidelines for effective and efficient data extraction in systematic reviews in software engineering". In: *ACM International Conference Proceeding Series*, pp. 170–179.

Garousi, Vahid, Michael Felderer, and Mika V. Mäntylä (2019). "Guidelines for including grey literature and conducting multivocal literature reviews in software engineering". In: *Information and Software Technology* 106.May 2018, pp. 101–121. ISSN: 09505849.

Goguen, Joseph A and Charlotte Linde (1993). "Techniques for requirements elicitation". In: *[1993] Proceedings of the IEEE International Symposium on Requirements Engineering*. IEEE, pp. 152–164.

Guggenberger, Tobias Moritz et al. (2020). "Ecosystem Types in Information Systems". In: *Twenty-Eighth European Conference on Information Systems (ECIS)*, pp. 1–21.

Gustafsson, Johanna (2017). "Single case studies vs. multiple case studies: A comparative study". In: *Academy of Business, Engineering and Science Halmstad University, Sweden*, pp. 1–15.

Halpert, Benjamin (2004). "Mobile Device Security". In: *Proceedings of the 1st Annual Conference on Information Security Curriculum Development*. InfoSecCD '04. Kennesaw, Georgia: Association for Computing Machinery, 99–101. ISBN: 1595930485.

Hernandez-Ramirez, E. M., V. J. Sosa-Sosa, and I. Lopez-Arevalo (2012). "A comparison of redundancy techniques for private and hybrid cloud storage". In: *Journal of Applied Research and Technology* 10.6, pp. 893–901. ISSN: 16656423.

Hevner, Alan and Samir Chatterjee (2010). *Design Research in Information Systems*. Vol. 28, pp. 63–86. ISBN: 978-1-4419-5652-1.

Hogan, Michael et al. (2011). "NIST Cloud Computing Standards Roadmap". In: *Communications in Computer and Information Science* 3, pp. 1–6. ISSN: 18650929.

Hon, W. Kuan, Christopher Millard, and Ian Walden (2012). "Negotiating Cloud Contracts - Looking at Clouds from Both Sides Now". In: *SSRN Electronic Journal*, pp. 81–130.

IT Governance Publishing, Privacy Team (2017). *EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide - Second edition*. ISBN: 9781849288354.

Jansen, Slinger, Michael Cusumano, and Karl Michael Popp (2019). "Managing software platforms and ecosystems". In: *IEEE Software* 36.3, pp. 18–21. ISSN: 19374194.

Jarke, Matthias et al. (1993). "Theories underlying requirements engineering: An overview of nature at genesis". In: *Proceedings of the IEEE International Conference on Requirements Engineering* February, pp. 19–31.

Jeon, Hangoo and Kwang Kyu Seo (2015). "A Framework and Improvements of the Korea Cloud Services Certification System". In: *Scientific World Journal*. ISSN: 1537744X.

Kabbedijk, Jaap et al. (2014). "Defining Multi-Tenancy : A Systematic Mapping Study on the Academic and the Industrial Perspective". In: pp. 1–28.

Kaur, Gurpreet and Rajesh Kumar (2015). "A Review on Reliability Issues in Cloud Service". In: *International Journal of Computer Applications*.

Khoshkholghi, Mohammad Ali et al. (2014). "Disaster Recovery in Cloud Computing: A Survey". In: *Computer and Information Science* 7.4, p. 39. ISSN: 1913-8989.

Kitchenham, Barbara (2004). "Procedures for Performing Systematic Reviews". In: ISSN: 1353-7776.

Kumar, P. Ravi, P. Herbert Raj, and P. Jelciana (2018). “Exploring Data Security Issues and Solutions in Cloud Computing”. In: *Procedia Computer Science*, pp. 691–697. ISSN: 18770509.

Ma, Dan (2007). “The business model of "Software-as-a-Service"”. In: *IEEE International Conference on Services Computing SCC 2007*. July. Salt Lake City, pp. 701–702.

Mäkilä, Tuomas et al. (2010). “How to Define Software-as-a-Service - An Empirical Study of Finnish SaaS Providers”. In: *Software Business*. Vol. 51, pp. 115–124. ISBN: 978-3-642-13632-0.

Mesbahi, Mohammad Reza, Amir Masoud Rahmani, and Mehdi Hosseinzadeh (2018). “Reliability and high availability in cloud computing environments: a reference roadmap”. In: *Human-centric Computing and Information Sciences* 8.1. ISSN: 21921962.

Moravcik, Marek, Pavel Segec, and Martin Kontsek (2018). “Overview of Cloud Computing Standards”. In: *ICETA 2018 - 16th IEEE International Conference on Emerging eLearning Technologies and Applications, Proceedings*. November, pp. 395–402. ISBN: 9781538679142.

Najjar, Sireen Kamal and Khalid T. Al-Sarayreh (2015). “Capability maturity model of Software requirements process and integration (SRPCMMI)”. In: *ACM International Conference Proceeding Series* 23-25-November-2015, pp. 1–5.

Ojala, Arto (2012). “Comparison of different revenue models in SaaS”. In:

Olivé, Antoni (2007). *Conceptual Modeling of Information Systems*.

Osborn, Alex F (1953). “Applied imagination. Charles Scribner’s Sons”. In:

Palos-Sanchez, Pedro R. (2017). “Drivers and Barriers of the Cloud Computing in SMEs: the Position of the European Union”. In: *Harvard Deusto Business Research*. ISSN: 2254-6235.

Patton, M (2015). *Qualitative research & evaluation methods*. 4th. Thousand Oaks.

Pauley, Wayne (2010). “Cloud provider transparency: An empirical evaluation”. In: *IEEE Security and Privacy* 8.6, pp. 32–39. ISSN: 15407993.

Pöttering, H. G. and J. Lenarčič (2008). “Regulation (EC) no 593/2008 of the European parliament and of the council of 17 june 2008 on the law applicable to contractual obligations (Rome I)”. In: *Official Journal of the European Union*.

Pourshahid, Alireza et al. (2007). “Business process monitoring and alignment: An approach based on the user requirements notation and business intelligence tools”. In: *Proceedings of the 10th Workshop on Requirements Engineering, WER 2007*, pp. 80–91.

Prat, Nicolas, Isabelle Comyn-Wattiau, and Jacky Akoka (2015). “A Taxonomy of Evaluation Methods for Information Systems Artifacts”. In: *Journal of Management Information Systems* 32.3, pp. 229–267. ISSN: 1557928X.

Pries-Heje, Jan, Richard Baskerville, and John Venable (2008). “Strategies for design science research evaluation”. In: *16th European Conference on Information Systems, ECIS 2008*.

Purchase, Helen C. et al. (2003). “UML Class Diagrams: An Empirical Study of Comprehension”. In: *Software Visualization* 9.December, pp. 149–178.

Rotondo, Elisabetta (2013). “The legal effect of EU Regulations”. In: *Computer Law and Security Review* 29.4, pp. 437–445. ISSN: 02673649.

Runeson, Per and Martin Höst (2009). “Guidelines for conducting and reporting case study research in software engineering”. In: *Empirical Software Engineering* 14.2, pp. 131–164. ISSN: 13823256.

Sabbaghi, Fatemeh, Arash Mahboubi, and Siti Hajar Othman (2017). “Hybrid Service for Business Contingency Plan and Recovery Service as a Disaster Recovery

Framework for Cloud Computing". In: *Journal of Soft Computing and Decision Support Systems* 4.4, pp. 1–10. ISSN: 2289-8603.

Salleh, Noor Afzan et al. (2018). "A systematic literature review of cloud computing adoption and impacts among small medium enterprises (SMEs)". In: *Proceedings - International Conference on Information and Communication Technology for the Muslim World 2018, ICT4M 2018*, pp. 278–284.

Saquib, Zia et al. (2013). "A new approach to disaster recovery as a service over cloud for database system". In: *2013 15th International Conference on Advanced Computing Technologies (ICACT)*, pp. 1–6.

Schneider, Stephan et al. (2014). "A taxonomic perspective on certification schemes: Development of a taxonomy for cloud service certification criteria". In: *Proceedings of the Annual Hawaii International Conference on System Sciences*, pp. 4998–5007. ISSN: 15301605.

Schulz, M and I Korčok (2016). "Directive (EU) 2016/ 1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union". In: *Official Journal of the European Union* 6.1, p. 30.

Shanthan, Samuel (2016). "Ensuring Vendor Continuity". In: *ISACA Journal* 3, pp. 1–5.

Shrestha, Anup, Aileen Cater-steel, and Mark Toleman (2014). "How to Communicate Evaluation Work in Design Science Research ? An Exemplar Case Study". In: 2007.

Stanton, Ray (2005). "Beyond disaster recovery: The benefits of business continuity". In: *Computer Fraud and Security* 7, pp. 18–19. ISSN: 13613723.

Suguna, S. and A. Suhasini (2014). "Overview of data backup and disaster recovery in cloud". In: *2014 International Conference on Information Communication and Embedded Systems, ICICES 2014* 978.

Sun, Le et al. (2014). "Cloud service selection: State-of-the-art and future research directions". In: *Journal of Network and Computer Applications* 45, pp. 134–150. ISSN: 10958592.

Sunyaev, Ali and Stephan Schneider (2013). "Cloud Services Certification". In: *Communications of the ACM* 56.2, pp. 33–36. ISSN: 00010782.

Tajani, A and G Ciamba (2019). "Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation". In: *Official Journal of the European Union* 2019.L151/15, pp. 15–69.

Tang, Changlong and Jiqiang Liu (2015). "Selecting a trusted cloud service provider for your SaaS program". In: *Computers and Security* 50, pp. 60–73. ISSN: 01674048.

Torabi, S. A., H. Rezaei Soufi, and Navid Sahebjamnia (2014). "A new framework for business impact analysis in business continuity management (with a case study)". In: *Safety Science* 68, pp. 309–323. ISSN: 18791042.

Tsai, Wei Tek, Xin Sun, and Janaka Balasooriya (2010). "Service-oriented cloud computing architecture". In: *ITNG2010 - 7th International Conference on Information Technology: New Generations*, pp. 684–689.

Turley, Gerard, Geraldine Robbins, and Stephen McNena (2015). "A Framework to Measure the Financial Performance of Local Governments". In: *Local Government Studies* 41.3, pp. 401–420. ISSN: 17439388.

Tweneboah-Koduah, Samuel and William J. Buchanan (2018). "Security risk assessment of critical infrastructure systems: A comparative study". In: *Computer Journal* 61.9, pp. 1389–1406. ISSN: 14602067.

Unkelos-Shpigel, N., S. Sherman, and I. Hadar (2015). "Finding the Missing Link to Industry: LinkedIn Professional Groups as Facilitators of Empirical Research". In: *2015 IEEE/ACM 3rd International Workshop on Conducting Empirical Studies in Industry*, pp. 43–46.

Van De Zande, Tommy and Slinger Jansen (2011). "Business continuity solutions for SaaS customers". In: *Lecture Notes in Business Information Processing* 80 LNBIP, pp. 17–31. ISSN: 18651348.

Vaquero, LM et al. (2009). "A Break in the Clouds: Towards a Cloud Definition". In: *ACM SIGCOMM Computer Communication Review* 39, pp. 50–55.

Venable, John Robert, Jan Pries-heje, and Richard Baskerville (2012). "Design Science Research in Information Systems. Advances in Theory and Practice". In: May.

Wang, Zhan et al. (2013). "Verification of data redundancy in cloud storage". In: *Cloud Computing 2013 - Proceedings of the 2013 International Workshop on Security in Cloud Computing*, pp. 11–18.

Weerd, Inge van de and Sjaak Brinkkemper (2008). "Meta-modeling for situational analysis and design methods". In: *Handbook of Research on Modern Systems Analysis and Design Technologies and Applications*, pp. 35–54.

Weigl, Elisabeth, Johannes Binder, and Stephan Strodl (2013). "A Framework for Automated Verification in Software Escrow". In: *Proceedings of the 10th International Conference on Preservation of Digital Objects*, pp. 95–103. ISBN: 9789725654934.

Wessel, Ramses A (2015). "Towards EU cybersecurity law: Regulating a new policy field". In: *Research Handbook on International Law and Cyberspace*. Edward Elgar Publishing.

Wiboonrat, Montri and Kitti Kosavisutte (2008). "Optimization strategy for disaster recovery". In: *Proceedings of the 4th IEEE International Conference on Management of Innovation and Technology, ICMIT*, pp. 675–680.

Wieringa, Roel J. (2014). *Design science methodology: For information systems and software engineering*, pp. 1–332. ISBN: 9783662438398.

Wohlin, Claes (2014). "Guidelines for snowballing in systematic literature studies and a replication in software engineering". In: *ACM International Conference Proceeding Series*.

Yin, R. K. (1994). "Case Study Research: Design and Methods". In: 2nd.

Yu, Shucheng, Kui Ren, and Wenjing Lou (2012). "Data Security in Cloud Computing". In: *Handbook on Securing Cyber-Physical Critical Infrastructure*. 1st. Chap. 15.

Zave, Pamela (1997). "Classification of research efforts in requirements engineering". In: *ACM Computing Surveys (CSUR)* 29.4, pp. 315–321.

Zowghi, Didar and Chad Coulin (2005). "Requirements elicitation: A survey of techniques, approaches, and tools". In: *Engineering and Managing Software Requirements*, pp. 19–46.

Grey Literature

Audit, Information Systems and Control Association (2012). *Business Continuity Management: Emerging Trends*. URL: https://www.isaca.org/bookstore/bookstore-wht_papers-digital/whpbcm (visited on 01/28/2020).

Balkhi, Syed (2018). *How to Network on LinkedIn Like a Pro*. URL: https://www.business.com/articles/linkedin-networking-tips/ (visited on 05/14/2020).

Barreira, Inigo et al. (2019). *Standards Supporting Certification - Analysis of Standards in Areas Relevant to the Potential EU Candidate Cybersecurity Certification Schemes*. Tech. rep. ENISA. URL: https://www.enisa.europa.eu/publications/recommendations-for-european-standardisation-in-relation-to-csa-ii (visited on 02/15/2020).

Baudoin, Claude et al. (2016). *Cloud Security Standards : What to Expect & What to Negotiate Version 2.0*. Tech. rep. Cloud Standards Customer Council, pp. 1–36. URL: https://www.omg.org/cloud/deliverables/CSCC-Cloud-Security-Standards-What-to-Expect-and-What-to-Negotiate.pdf (visited on 03/14/2020).

Bendiek, Annegret and Martin Schallbruch (2019). *Europe ' s Third Way in Cyberspace*. URL: https://www.swp-berlin.org/10.18449/2019C52/.

Bessemer Venture Partners et al. (2020). *State of the Cloud*. Tech. rep. Partners Bessemer Venture. URL: http://www.jackofallclouds.com/2011/01/state-of-the-cloud-january-201/.

Board of Governors of the US Federal Reserve System (2018). *What is financial stability?* URL: https://www.federalreserve.gov/faqs/what-is-financial-stability.htm (visited on 03/01/2019).

Boruvka, John (2016). *What contract risks are hiding in the cloud?* URL: https://journal.iaccm.com/contracting-excellence-journal/iaccm-member-articles/what-contract-risks-are-hiding-in-the-cloud (visited on 02/04/2020).

Carey, Mark et al. (2013). *Special Purpose Vehicles and Securitization*. URL: https://www.nber.org/chapters/c9619.pdf (visited on 01/14/2020).

Catteddu, Daniele and Giles Hogben (2009). *Cloud Computing: Benefits, risks and recommendations for information secuirty*. Tech. rep. ENISA. URL: https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security (visited on 01/16/2020).

Cloud Secuirty Alliance (2014). *loud Security Alliance Cloud Consensus Assessments Initiative Questionnaire v3.0.1*. URL: https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v3-0-1/ (visited on 02/02/2020).

Cloud Security Alliance (2017a). *CSA Security Guidance v4*. Tech. rep., p. 152. URL: https://cloudsecurityalliance.org/download/security-.

— (2017b). *D3.5 Risk-based decision making mechanisms for cloud service (Final report)*. Tech. rep. URL: http://www.cloudwatchhub.eu/sites/default/files/CloudWATCH2{_}Risk-based-decision-making-mechanisms-for-cloud-services.pdf (visited on 01/23/2020).

CloudWatch2 (2017). *The Cloud Standards Guide*. URL: http://www.cloudwatchhub.eu/cloud-standards-guide (visited on 03/17/2020).

CompTIA (2019). *Quick Start Guide to Business Continuity and Data Recovery*. Tech. rep. URL: https://www.comptia.org/content/guides/comptia-quick-start-guide-to-business-continuity-and-data-recovery (visited on 12/08/2020).

De Jong, Marco, Slinger Jansen, and Sietse Overbeek (2019). *Critical Applications Should Come With Critical Questions : Business Continuity Solution Adoption at Dutch SaaS-Providers*. URL: https://saas-continuiteit.nl/wp-content/uploads/2019/11/deJong_5704367-OZP_SaaS_Business_Continuity-August_1_2019.pdf (visited on 11/25/2019).

Elliott, Rachael, Catherine Thomas, and Kamal Muhammad (2020). *BCI Horizon Scan Report 2020*. Tech. rep. 40. BSI. URL: https://www.bsigroup.com/localfiles/en-gb/iso-22301/resources/bci-horizon-scan-report-2020.pdf (visited on 04/30/2020).

EscrowTech (n.d.). *Software Escrow Fundamentals: The ins and outs of Software Escrows, Source Code Escrows and Technology Escrows*. URL: https://www.escrowtech.com/software-escrow.php (visited on 02/06/2020).

European Commision (2003). *Internal Market, Industry, Entrepreneurship and SMEs: What is an SME?* URL: https://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition{_}en (visited on 02/26/2020).

Expedited SSL Inc (2020). *API Security Best Practices MegaGuide*. URL: https://expeditedsecurity.com/api-security-best-practices-megaguide/.

Gagnaire, M et al. (2012). *Downtime statistics of current cloud solutions*. Tech. rep. March, pp. 2–4. URL: http://iwgcr.org/wp-content/uploads/2012/06/IWGCR-Paris.Ranking-002-en.pdf (visited on 01/15/2020).

Goel, Sandeep (2015). *Financial ratios*. URL: https://ebookcentral.proquest.com (visited on 03/06/2020).

Habil, Nizar Abdelkafi et al. (2018). *Understanding ICT Standardization: Principles and Practice*. URL: https://www.etsi.org/images/files/Education/Understanding{_}ICT{_}Standardization{_}LoResPrint{_}20190125.pdf (visited on 04/16/2020).

Hayes, Adam (2019a). *Asset Turnover Ratio Definition*. URL: https://www.investopedia.com/terms/a/assetturnover.asp (visited on 02/06/2020).

— (2019b). *Debt Ratio Definition*. URL: https://www.investopedia.com/terms/d/debtratio.asp (visited on 02/06/2020).

— (2019c). *Debt-Service Coverage Ratio*. URL: https://www.investopedia.com/terms/d/dscr.asp (visited on 02/06/2020).

ISO (2019). *ISO 22301:2019(en) Security and resilience — Business continuity management systems — Requirements*. URL: https://www.iso.org/obp/ui/{\#}iso:std:iso:22301:ed-2:v1:en (visited on 02/04/2020).

ITPro (2008). *Cloud Storage Service Loses Data, Shuts Down*. URL: https://www.itprotoday.com/storage/cloud-storage-service-loses-data-shuts-down (visited on 02/07/2020).

Jansen, Wayne and Timothy Grance (2011). *Guidelines on Security and Privacy in Public Cloud Computing*. Tech. rep. National Institute of Standards and Technology. URL: https://www.leica-microsystems.com/science-lab/topics/multiphoton-microscopy/ (visited on 01/23/2020).

Jayachandran, Janaki (2014). *Can a multi-tenant framework offer benefits of both IaaS and PaaS?* URL: https://blog.techcello.com/can-a-multi-tenant-framework-offer-benefits-of-both-iaas-and-paas/ (visited on 02/27/2020).

Kenton, Will (2019a). *Current Ratio*. URL: https://www.investopedia.com/terms/c/currentratio.asp (visited on 02/06/2020).

Kenton, Will (2019b). *Operating Cash Flow Margin*. URL: https://www.investopedia.com/terms/o/operating-cash-flow-margin.asp (visited on 02/06/2020).

— (2019c). *Operating Margin Definition*. URL: https://www.investopedia.com/terms/o/operatingmargin.asp (visited on 02/06/2020).

— (2019d). *Quick Ratio Definition*. URL: https://www.investopedia.com/terms/q/quickratio.asp (visited on 02/06/2020).

— (2019e). *Return on Capital Employed*. URL: https://www.investopedia.com/terms/r/roce.asp (visited on 02/06/2020).

Kosutic, Dejan (2015). *Information security & business continuity standards*. URL: https://advisera.com/27001academy/knowledgebase/information-security-business-continuity-standards/ (visited on 03/27/2020).

Lawrence, Amanda et al. (2014). *Where is the evidence: realising the value of grey literature for public policy and practice*. URL: https://researchbank.swinburne.edu.au/file/8546f00c-f178-48e6-bf86-cd04d0907bef/1/PDF\%20\%28Published\%20version\%29.pdf (visited on 12/15/2019).

Leteinturier, Aurelien et al. (2019). *CSPCERT WG (Milestone 3) Recommendations for the implementation of the CSP Certification scheme*. Tech. rep. CSPCERT WG. URL: https://drive.google.com/file/d/1J2NJt-mk2iF{_}ewhPNnhTywpo0zOVcY8J/view (visited on 02/15/2020).

Lomas, Akash (2014). *What is Google App Engine, Its Advantages and How it Can Benefit Your Business*. URL: https://www.netsolutions.com/insights/what-is-google-app-engine-its-advantages-and-how-it-can-benefit-your-business/.

Martin, James and John Waters (2018). *What is IAM? Identity and access management explained*. URL: https://www.csoonline.com/article/2120384/what-is-iam-identity-and-access-management-explained.html.

Maverick, J.B (2016). *What Is the Best Measure of a Company's Financial Health?* URL: https://www.investopedia.com/articles/investing/061916/what-best-measure-companys-financial-health.asp (visited on 02/29/2020).

Mell, Peter and Timothy Grance. Tech. rep. URL: http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf.

Murphy, Chris (2019a). *Accounts Payable Turnover Ratio Definition*. URL: https://www.investopedia.com/terms/a/accountspayableturnoverratio.asp (visited on 02/06/2020).

— (2019b). *Receivables Turnover Ratio*. URL: https://www.investopedia.com/terms/r/receivableturnoverratio.asp (visited on 02/06/2020).

— (2020). *Net Profit Margin*. URL: https://www.investopedia.com/terms/n/net_margin.asp (visited on 02/06/2020).

Newman, Lily Hay (2020). *The Covid-19 Pandemic Reveals Ransomware's Long Game*. URL: https://www.wired.com/story/covid-19-pandemic-ransomware-long-game/ (visited on 05/14/2020).

ORACLE and KPMG (2020). *Oracle and KPMG Cloud Threat Report, 2020*. Tech. rep., p. 41. URL: https://www.oracle.com/a/ocom/docs/dc/final-oracle-and-kpmg-cloud-threat-report-2019.pdf?elqTrackId=063c9f4a2a5b465ab55b734007a900f0{\&}elqaid=79797{\&}elqat=2.

Patel, Pankesh, Ajith H. Ranabahu, and Amit P. Sheth (2009). *Service Level Agreement in Cloud Computing*. URL: https://corescholar.libraries.wright.edu/knoesis/78/{\%}0Ahttps://works.bepress.com/amit{_}sheth/14/ (visited on 01/15/2020).

Phillips, Brenda D. (2009). *Disaster recovery 101*. Tech. rep. Zerto. URL: https://www.zerto.com/page/disaster-recovery-101/.

Preez, Derek du (2015). *A CIO's worst nightmare: When your cloud provider goes bankrupt*. URL: https://diginomica.com/cios-worst-nightmare-cloud-provider-goes-bankrupt (visited on 02/08/2020).

Quinton, Sarah and Damien Wilson (2016). *Tensions and ties in social media networks: Towards a model of understanding business relationship development and business performance enhancement through the use of LinkedIn*. URL: http://dx.doi.org/10.1016/j.indmarman.2015.12.001 (visited on 05/12/2020).

Rutherford, Robert (2019). *How does the cloud and SaaS affect business continuity planning?* URL: https://www.quostar.com/blog/considering-bcp-in-relation-to-cloudsaas/ (visited on 02/13/2020).

Rzepka, Sebastian (2012). *Overview: Data encryption in SaaS applications*. URL: https://www.ibm.com/blogs/cloud-computing/2012/06/19/what-about-data-encryption-in-saas-applications/.

Sagastume, Jorge (2017). *How To Choose A SaaS Escrow Service and Ensure Business Continuity*. URL: https://dzone.com/articles/how-to-choose-a-saas-escrow-service-and-provide-bu (visited on 02/06/2020).

Snedaker, Susan and Chris Rima (2013). *Business continuity and disaster recovery planning for IT professionals*. URL: https://books.google.tt/books?hl=en{\&}lr={\&}id=vT8TAAAAQBAJ{\&}oi=fnd{\&}pg=PP1{\&}dq=define+business+continuity{\&}ots=d0Awl9268-{\&}sig=bbSNwGjVXDweTGpLChMpQ0gnBww{\&}redir{_}esc=y{\#}v=onepage{\&}q=definebusinesscontinuity{\&}f=false (visited on 03/09/2020).

Stulman, John J (2008). *Technology Escrow Agreements and Software-as-a-Service*. URL: http://www.innovasafe.com/pdf/TechnologyEscrowandSaaS.pdf (visited on 01/23/2020).

The Cloud Service Measurement Initiative Consortium (CSMIC) (2014). *Service Measurement Index Introducing the Service Measurement Index (SMI)*. Tech. rep. Carnegie Mellon University, pp. 1–8. URL: http://www.cloudcommons.com/about-smi (visited on 12/15/2020).

TUDelft (2019). *Template Informed Consent Form [Website]*. URL: https://www.tudelft.nl/over-tu-delft/strategie/integriteitsbeleid/human-research-ethics/template-informed-consent-form/.

Van Velzen, Denise, Marco De Jong, and Slinger Jansen (2019). *Business Continuity Risks Through the Use of Software-As-A-Service : A Descriptive Survey*. URL: https://saas-continuiteit.nl/wp-content/uploads/2019/11/vanVelzen-5493994-OZPSaaSContinuity-CompleteV2.pdf (visited on 11/23/2019).

Zeker-Online (2016). *Framework of Standards Legal requirements Infrastructure Application – Generic and Specific accounting services*. URL: https://www.zeker-online.nl/wp-content/uploads/2018/03/framework-of-standards-zeker-online-english-version-3.1-legal-infra-and-generic-and-specific-accounting-application.pdf (visited on 12/13/2019).

— (2019). *Trust in onlines services*. URL: https://www.zeker-online.nl/partneringtrust/ (visited on 02/03/2020).