

# MASTER'S THESIS

## The impact of the use of SAAS Cloud Computing on the Enterprise Security Architecture

Mulkens, E.

**Award date:**  
2021

[Link to publication](#)

### General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain.
- You may freely distribute the URL identifying the publication in the public portal.

### Take down policy

If you believe that this document breaches copyright please contact us at:

[pure-support@ou.nl](mailto:pure-support@ou.nl)

providing details and we will investigate your claim.

Downloaded from <https://research.ou.nl/> on date: 12. Dec. 2021

**Open Universiteit**  
[www.ou.nl](http://www.ou.nl)



# De impact van het gebruik van SAAS Cloud Computing op de Enterprise Security Architecture

## The impact of the use of SAAS Cloud Computing on the Enterprise Security Architecture

Institute: Open Universiteit, faculteit Betawetenschappen  
Masteropleiding Business Process Management & IT

Degree programme: Open University of the Netherlands, Faculty of Science  
Master of Science Business Process Management & IT

Course: IM0602 BPMIT Graduation Assignment Preparation  
IM9806 Business Process Management and IT Graduation Assignment

Student: E. Mulkens

Identification number:

Date: 01-09-2021

Thesis supervisor dr. Rik Bos

Second reader ir. L. Cuijpers

Version number: 1.0

Status: AF final version

## Abstract

Recent studies have provided information on usage of Enterprise Security Architecture and related risk and security controls in a Cloud Computing environment in general, but less concerning the deployment of Enterprise Security Architecture within a Software As A Service Cloud Computing service model.

The purpose of this study is to explore to what extent Enterprise Security Architecture can be used to map/model risk and security controls in a Software As A Service Cloud Computing service model from a Cloud Service Customer point of view.

To answer this research question, an exploratory and descriptive, holistic multi-case study approach was adopted. Data is collected by conducting a combined method of survey and semi-structured interview with key stakeholders of selected Small and Medium sized Enterprises.

Research findings show that Cloud Service Providers will cover many aspects of physical, infrastructure, and application security elements while Cloud Service Customers remains responsible for certain areas of security and control like compliance, user access and data. Cloud Service Customers can use Enterprise Security Architecture to manage the areas of security and risk control for which they remain responsible, although Enterprise Security Architecture is only used to a very limited extend within Small and Medium sized Enterprises.

## Key Terms

Enterprise Security Architecture (ESA), Cloud Computing, Software as a Service (SAAS), Small and Medium sized Enterprise (SME)

## Summary

Risk and security controls are high priority within enterprises. Currently a lot of organizations are using CC concepts or are interested in using them, but it is not clear what the impact is on the Enterprise Security Architecture (ESA) and how this should reflect the risk and security controls. During the research we investigated to what extent ESA can be used to map/model risk and security controls in a Software As A Service (SAAS) Cloud Computing (CC) service model from a Cloud Service Customer (CSC) point of view. This research was limited to the SAAS CC service model within Small and Midsize Enterprises (SME).

From literature research we found that literature on this topic was mostly based on CC in general. Only limited literature was found on this topic with regards to the SAAS CC service model specifically. Based on the literature research outcome, a limited set of risk- and security elements were deducted for further investigation. In addition, our research only found a limited number of documents on the topic of the deployment of ESA for modelling/mapping risk and security related elements in a SAAS CC service model.

The follow up research was based on a concurrent mixed method approach. The use of the mixed method allowed both sets of results to be interpreted together, which provided a richer and more comprehensive response to the research question in comparison to the use of a mono method design. In addition, the mixed method was used in order to combine data to ascertain if the findings from one method mutually corroborate the findings from the other method.

From results it was recognized that researched SMEs did not hesitate in using SAAS applications, as they relied on the compliance information from the SAAS providers. SAAS applications did have policies and guidelines for authorization, authentication and identification, but there were also some exceptions. Confidence in the availability of the SAAS application was high, but there was no up to date insights in vulnerabilities and threats. There was no insight in the technical and logical architecture of the SAAS application. This was limited to encryption and security protocols only. Researched SMEs showed that there was no ESA governance setup and that there was only a limited budget available for security and risk issues.

SAAS Customers should use ESA to identify the risks of utilizing the SAAS service model. Trust of the SAAS customer in the area of compliance of SAAS providers is high, but no ESA is in place to check and confirm on this trust. The CSC can use ESA artifacts, such as tools and methods to guarantee and monitor compliance. SAAS customers have confidence in authentication and identification methods, but these are not always secure enough. This has an impact on risk and security controls. Identification, authentication and authorization can be setup and monitored with ESA. SAAS customers have no up-to-date insights in security vulnerabilities and detected threats. They completely rely on the CSP (Cloud Service Provider) for monitoring and controlling, and ESA cannot be used from CSC point of view. SAAS customers have no insights in technical and logical architecture of SAAS applications architecture and they cannot gain insight in the possible vulnerabilities. The CSC can't use ESA to implement the controls needed to manage the security. These controls are the responsibility of the SAAS provider. ESA is deployed to a limited extent by the CSC. In none of the researched organizations there was a governance setup nor a dedicated security

architect. A small budget for risk management and the limited use of ESA in general, prevents extensive deployment of ESA for a CSC in a SAAS CC service model.

Both, CSP and the CSC, have shared responsibility in securing the cloud and minimizing the risk, but shared responsibility does not mean less responsibility. CSPs will cover many aspects of physical, infrastructure, and application security while CSCs remains responsible for certain areas of security and control like compliance, user access and data. CSCs can use ESA to manage the areas of security and risk control for which they remain responsible. But the current limited use of ESA within SMEs provides a poor basis for managing it in a SAAS CC service model.

# Contents

Abstract .....	ii
Key Terms.....	ii
Summary .....	iii
Contents.....	v
1. Introduction .....	1
1.1. Background .....	1
1.2. Exploration of the topic .....	1
1.3. Problem statement .....	3
1.4. Research objective and questions .....	3
1.5. Motivation/relevance .....	4
1.6. Main lines of approach .....	4
2. Theoretical framework .....	5
2.1. Research approach.....	5
2.2. Implementation .....	6
2.3. Results and conclusions .....	7
2.4. Objective of the follow-up research .....	8
3. Methodology.....	10
3.1. Conceptual design: select the research method(s) .....	10
3.2. Technical design: elaboration of the method.....	11
3.3. Data analysis .....	12
3.4. Reflection w.r.t. validity, reliability and ethical aspects .....	14
4. Results.....	17
4.1. Case organizations .....	17
4.2. Implementation of the research.....	17
4.2.1. Surveys .....	17
4.2.2. Interviews.....	18
4.3. Results.....	18
4.3.1. Compliance and Regulation .....	18
4.3.2. Identification, Authentication and Authorization.....	19
4.3.3. Operational maintenance and Administration .....	20
4.3.4. Architecture .....	21
4.3.5. Deployment of ESA in a SAAS service model .....	22

5. Discussion, conclusions and recommendations .....	23
5.1. Discussion – reflection and limitations .....	23
5.1.1. Discussion - reflection .....	23
5.1.2. Discussion - limitations .....	26
5.2. Conclusions .....	27
5.3. Recommendations for practice.....	30
5.4. Recommendations for further research .....	30
References.....	31
Abbreviations .....	34
Appendix A: Overview of case organization .....	35
Appendix B: Overview of respondents .....	36
Appendix C: Survey/Interview information - protocol.....	37
Appendix D: Survey/Interview questions template .....	40
Appendix E: Survey score .....	50
Appendix F: Determination of similarities/differences and common themes.....	53
Appendix G: Theme count.....	64

# 1. Introduction

## 1.1. Background

The introduction of Cloud Computing (CC) transformed the traditional IT landscape. CC changes the way IT is provisioned and used. CC has many advantages and can lower the barriers for IT innovation.

Some of the benefits of CC are avoiding big initial investments for hardware and software acquisition, reduction of operational and maintenance costs, achieving better capacity utilization, pay per use, high availability of various software applications and achieving business agility (Motahari-Nezhad, Stephenson, and Singhal 2009).

On the other hand, the concept of CC brings many challenges and changes to the notion of system and data with regards to geographical distribution and control of the IT landscape. These challenges and changes relate to different topics like data governance, service management, process monitoring, infrastructure reliability, information security, data integrity and business continuity (Mahmood 2011). Moving a company's sensitive data into the hands of cloud providers expands and complicates the risk landscape in which the organization operates (Tang and Liu 2015).

Enterprise Architecture (EA), including Enterprise Security Architecture (ESA), is all about aligning business systems and supporting information systems to realize business goals in an effective and efficient manner. One of the important aspects of an EA is risk regarding information security and the way this can be managed. This research focuses on the role that ESA can play in determining the impact of risk and security within a CC environment.

In the next section of this chapter, we will explore the research area, the problem statement, the research objective and the research questions.

## 1.2. Exploration of the topic

### **Cloud computing**

According to NIST, CC is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (Mell and Grance 2011). This cloud model is composed of five essential characteristics, three service models, and four deployment models. The essential characteristics of CC are on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service. The different service models for CC are Software As A Service (SAAS), Platform As A Service (PAAS) and Infrastructure As A Service (IAAS).



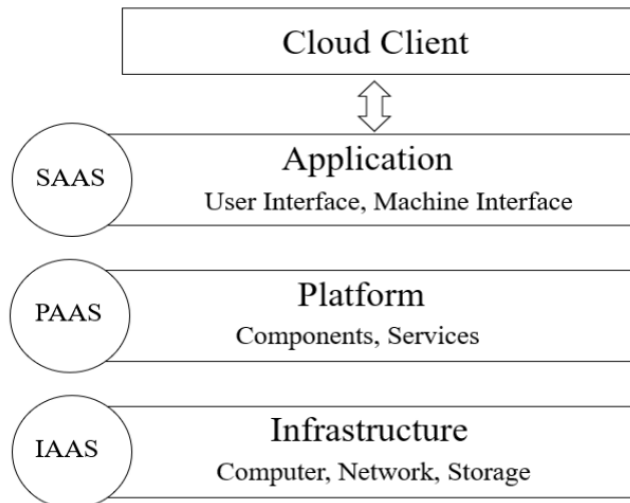


Figure 1 Cloud Computing service models

Deployment of CC is done via different models:

Private cloud, where the cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). Community cloud, where the cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). Public cloud, where the cloud infrastructure is provisioned for open use by the general public. Hybrid cloud, where the cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability.

### **Enterprise Architecture & security**

According to (Ahlemann, Stettiner, Messerschmidt, and Legner 2012), architecture is defined as the ‘fundamental organization of a system, embodied in its components, their relationships to each other and the environment, and the principles governing its design’. EA is therefore understood as the fundamental organization of an enterprise as a socio-technical system, along with the principles governing its design and development. An EA includes all relevant components for describing an enterprise, including its business and operating model, organizational structure, business processes, data, applications and technology. EA’s design rules provide stipulations for the development and structuring of the components, as well as a means to ensure consistency in the use of components and in their relationships. EAM (Enterprise Architecture Management) enables EA. EAM is defined as: “A management practice that establishes, maintains, and uses a coherent set of guidelines, architecture principles and governance regimes that provide direction for and practical help with the design and development of an enterprise’s architecture in order to achieve a vision and a strategy” (Ahlemann et al. 2012). Moving a company's sensitive data into the hands of cloud providers expands and complicates the risk landscape in which the organization operates (Tang and Liu 2015).

EA includes security architecture and is all about aligning business systems and supporting information systems to realize business goals in an effective and efficient manner (systems being the combination of processes, people, and technology). One of the important aspects of an EA is risk regarding information security and the way this can be managed. For too long, information security

has been considered a separate discipline, isolated from the EA (The Open Group, 2011). To be able to guarantee quality of service a structured information systems security architecture needs to be in place (Sherwood, Clark, and Lynas 2005).

### 1.3. Problem statement

CC is seeing an adoption and adaption across the globe. The CC idea is actually a smart and sensible combination of several proven and promising technologies (Mahmood & Hill, 2011).

Bringing cloud capabilities to an enterprise is about more than just the latest technology. It is about changing the traditional business and collaboration model with partners, customers, and providers of services to the enterprise. It is much more important for companies to understand the changing trends in business and their impacts on EA than to just implement the next “hot” technology product. The enterprise architect has a lot to do in helping enterprises define the best strategy to leverage the blooming and booming cloud models. Organizations are interested in using cloud solutions, but they are not clear on the impact on the EA. Enterprise Architects are being forced to tailor EA towards cloud-based solutions (Mahmood & Hill, 2011). And at the end this has to be done in a way that will minimize risk and maximize security for the organization.

Some of the main potential risks and security issues of CC within the enterprise are (Naresh Kumar, Pramod Chandra p, and John M 2020):

1. You lose direct knowledge and control of underlying hardware
2. Virtual Machine sharing the same hardware can affect your performance
3. Hard to diagnose performance issues, due to limited visibility and virtualization
4. Potential security risks of placing your mission critical data on remote servers
5. Vendor lock-in, means getting stuck with a Cloud provider who has your data

The general issue is that ESA mainly models only those computing and business components which are under the control of the enterprise. The characteristics and the business dynamics of CC have certainly changed the way enterprises use information systems. This requires enterprises tying their ESA together with the service characteristics of CC.

### 1.4. Research objective and questions

CC affects the EA (including the ESA) of an organization because part of the computer system resources is moved from within the organization to a cloud environment. This can be considered as a kind of “outsourcing”. One of the challenges here is to find a suitable architecture method that matches the characteristics of CC, such as the lack of direct knowledge and control of underlying hardware, managing visibility on performance and monitoring potential security risks and controls. The question is whether there are ESA frameworks that connect to this, and to what extent the existing ESA frameworks meet the cloud-specific conditions.

Goal of assignment/research:

In this research the impact of CC on the ESA is investigated. Risk and security implications result from the utilization of cloud-based solutions, and can be captured in the ESA. Goal of this research is to provide insight into the way in which ESA can be deployed for the adoption of a CC model. The focus of this research will be on SAAS, because SAAS is representing the largest cloud market and is also

considered to be the largest market segment for growth. Another reason to focus on only one cloud service model is the limited time available for conducting the research. The research was conducted from a Cloud Service Customer (CSC) point of view.

Main research question:

To what extent can ESA be used to map/model risk and security controls in a SAAS CC service model.

To be able to answer the main research question we need to investigate and answer following sub research questions:

1. Research Question 1 (RQ1): What is the impact of using the SAAS CC service model on risk and security controls.
2. Research Question 2 (RQ2): How is ESA being deployed in a SAAS CC service model.

## 1.5. Motivation/relevance

Risk and security controls are high priority within enterprises. Currently a lot of organizations are using CC concepts or are interested in using them, but it is not clear what the impact is on the ESA and how this should reflect the risk and security controls. As enterprises adopt Cloud-based solutions, more issues must be addressed and that makes ESA more complex. Enterprise Architects are being forced to tailor ESA towards Cloud-based solutions (Mahmood & Hill, 2011). Risk and security controls therefore need to be included as part of the ESA design for CC.

## 1.6. Main lines of approach

The steps that are followed to execute the research are handled in different chapters:

In Chapter 2 the theoretical framework is discussed and the sub-questions are investigated and answered.

Chapter 3 deals with the strategy, method and technique being used in the practical part of the research.

Chapter 4 contains the results of the practical research.

Chapter 5 contains the conclusion, discussion and recommendations. Finally in this chapter a reflection is given on the execution of the process for this research.

## 2. Theoretical framework

This chapter reviews the literature available on the use of the SAAS CC model and reflection of risk and security controls in the ESA. Based on this literature review the research approach, implementation, results and conclusions, objective and follow-up research are described.

### 2.1. Research approach

First of all, systematic literature search is used to find scientific literature on the use of risk and security controls within CC, and the possible impact on the ESA.

Because it was expected that there is a limited amount of literature to be found that has been peer-reviewed, also not-peer-reviewed articles have been searched for. This increased the chance of finding relevant information. The disadvantage is that not-peer-reviewed articles may lack a significant quality standard.

Search engines used:

Search engine	Entity	URL
Google Scholar	Google Inc.	<a href="https://scholar.google.nl/">https://scholar.google.nl/</a>
University Library	Open Universiteit	<a href="http://bibliotheek.ou.nl">http://bibliotheek.ou.nl</a>

The following search parameters were used in the queries of the different search engines.

Search queries parameters:

Parameter	Value
Language	Dutch, English
Search area	enterprise security architecture, cloud computing, SAAS, security
Date of publication	2012 - present
Type of Literature	Scientific, books, conference papers, master/PhD theses
Literature exclusion	Newspaper articles, book reviews

Only literature from 2012 – 2020 (present) is used for executing the search queries that are relevant for the literature research.

Furthermore, the snowballing method was used to find relevant literature. By using backward snowballing, it was possible to find literature by using a key document, and from there consult referenced documents. The disadvantage of this method is that it is searching retrospectively, so each source you find will be older than the previous one.

By using forward snowballing, it was possible to find documents referring to the key document (“cited by”).

The advantage of the snowballing method is that you are searching in a focused way. This increases chances of finding relevant information.

## 2.2. Implementation

Various combinations of search terms are used in the parameters for literature search and within the search engine. The main search is on ESA in combination with Cloud Computing (SAAS). Then a further focus is set to the area of security.

	Security	SAAS	Cloud Computing	Enterprise Security Architecture		Initial search results Google Scholar	Step 1: Inventory phase	Step 2: Global scan phase	Step 3: In-depth scan phase	Selected after Search/scan optimization and de-duplication
Search 1			x	x		185	10 (3)	8 (3)	6 (2)	5 (2)
Search 2		x	x	x		57	5 (2)	4 (2)	4 (2)	3 (1)
Search 3	x	x	x			23300	15 (3)	11 (3)	8 (1)	5 (1)
Search 4	x		x			309000	15 (5)	6 (3)	5 (2)	4 (2)
Search 5	x	x	x	x		1910	15 (2)	9 (2)	6 (1)	4 (1)
Total							60 (15)	38 (13)	29 (8)	21 (7)
(*) = peer reviewed										

Figure 2 Overview of search queries and results

There are three characteristics that determine whether or not a document was used for literature research:

- the relevance to the main question and sub-questions
- the recency of the document
- the quality of the document

The following steps were carried out:

1. Inventory phase: determine the relevance of a document on the basis of the title and short description and drop the document if the relevance is deemed too low.
2. Global scan phase: determine the relevance of the documents found from step 1 based on the introduction, conclusion and a global scan.
3. In-depth scan phase: Select the documents after affirmatively answering the questions:
  - a. Did the information answer (part of) my research question?
  - b. Did the information provide a good picture of the research topic?
  - c. Did the quality and level of the information match my needs?
  - d. Was there an overview of the sources used (bibliography)?

Only the documents remaining after step 3 were used for the literature research.

Some of the search queries gave a very large number of results. During search the search queries were optimized by using additional parameters:

- use more specific search terms
- add an extra search term to the search query (AND)
- search in specific search fields (title words, keywords)
- use limiters (e.g., between specific years, or peer-reviewed articles only)
- search for an exact phrase (use double quotation marks)

In Google Scholar the distinction whether articles were peer-reviewed or not, was not clear. In some cases, titles of relevant articles, found via this search engine, have also been entered into the online library of the Open Universiteit, in order to determine whether they were peer-reviewed.

## 2.3. Results and conclusions

To be able to answer this main research question we first need to investigate and answer the following sub research questions:

**Research Question 1 (RQ1):** What is the impact of using the SAAS CC service model on risk and security controls.

By using SAAS the customer is not able to manage and control the cloud infrastructure but is only able to configure some specific application parameters (Bouchaala, Ghazel, Saidane, and Kamoun 2017:303–10). The adoption of SAAS has some barriers, and one of the most significant barriers is security, followed by issues regarding compliance, privacy and legal matters (Hashizume, Rosado, Fernández-Medina, and Fernandez 2013). (Modi, Patel, Borisaniya, Patel, and Rajarajan 2013) concluded that since cloud services are delivered using classical network protocols and formats over the Internet, implicit vulnerabilities existing in these protocols, as well as threats introduced by newer architectures, raise many security and privacy concerns. Also (Niu, Liu, Zhang, Lü, and Li 2016) concluded that the number of security vulnerabilities in the cloud is more than in traditional enterprise services. (Sun 2018) mentions that SAAS introduces a new series of security concerns in three main security dimensions: computer security, network security and information security, and synthesizes a number of vital vulnerabilities and threats. Alam, S., Muqem, M., & Khan, S. A. (Alam, Muqem, and Khan 2018) use a classification model for identifying SAAS security issues and the relationship between vulnerabilities, attacks and threats. The impact of using SAAS on security and risk is significant and has been researched over the past years.

The search of the literature revealed that the number of security vulnerabilities and threats for SAAS is higher than for traditional enterprise services. The search of the literature also revealed limited attention has been paid to additional root causes that can have an impact on risk and security controls in SAAS environments, like vendor lock-in, jurisdiction/location of data and the use of SLAs.

Following risk and security key-elements have been deducted from the literature research (RQ1):

Nr	Element	Source
1	Compliance	(Modi et al. 2013), (Rath, Spasic, Boucart, and Thiran 2019), (Hashizume et al. 2013)
2	Regulation	(Modi et al. 2013),(Rath et al. 2019), (Hashizume et al. 2013)
3	Identification	(Bouchaala et al. 2017), (Rath et al. 2019)
4	Authentication	(Bouchaala et al. 2017), (Rath et al. 2019)
5	Authorization	(Bouchaala et al. 2017), (Rath et al. 2019)

6	Operational maintenance	(Hashizume et al. 2013), (Rath et al. 2019)
7	Administration	(Hashizume et al. 2013), (Rath et al. 2019)
8	Architecture	(Mahmood and Hill 2011), (Rath et al. 2019)

Table 1 risk and security elements

**Research Question 2 (RQ2):** How is ESA being deployed in a SAAS CC service model.

According to (Newcombe 2020) and (Hashizume et al. 2013) security is paramount in making the SAAS CC model successful. (Newcombe 2020) indicates that there are several benefits for implementing an ESA but that implementation should also handle responsibility for application security between customer and provider. (Hashizume et al. 2013) states that in a SAAS service model many more security services are delivered by the cloud service provider than in a IAAS or PAAS cloud service model. This is because of the degree of abstraction level (see Figure 1). The SaaS model is based on a higher degree of integrated functionality with minimal customer control. (Sherwood et al. 2005) developed a methodology for developing risk-driven enterprise information security and information assurance architectures that support critical business initiatives. It is an open standard, comprising a number of frameworks, models, methods and processes and can be aligned with cloud security standards such as ENISA (The European Commission 2020) , NIST (Nieles, Dempsey, and Pillitteri 2017) and CSA (Mogull, Arlen, Gilbert, Lane, Mortman, Peterson, and Rothman 2009) (Mahmood 2011) (Gonzalez, Miers, Redígolo, Carvalho, Simplicio, Näslund, and Pourzandi 2011). The CSA is considered as one of the most renown alliances for cloud security standards (Caballero 2020). The CSA Cloud Controls Matrix (CCM) is a security control framework for CC, composed of control objectives that are structured in different domains, covering all key aspects of the cloud technology. The controls framework is aligned to the CSA Security Guidance v4 (Mogull et al. 2009) and is currently considered a de-facto standard for cloud security assurance and compliance. (Rath et al. 2019) are using a five-step approach, starting with security requirements identification to security pattern classification. This pattern approach is a more comprehensive way of addressing security topics for CC. Another approach is mentioned by the National Cyber Security Center (Nationaal Cyber Security Center 2012) where a framework has been drawn up from a security point of view and describes specific security elements for CC.

There are different standards and security control frameworks that can be utilized for architecting security in CC environments, however from this literature review it is not recognized if there are specific ones for the SAAS model, how they differ from other cloud models and if they are utilized.

Our literature research only found a limited number of documents on the topic of the deployment of ESA for modelling/mapping risk and security related elements in a SAAS CC service model. Recent studies confirm that there is a currently lacking theoretical body of knowledge on EA-driven information security management practices and their practical implications that should be generally applicable (Larno, Seppänen, and Nurmi 2019).

This research also investigates the subject of how ESA is being deployed in a SAAS CC service model (RQ2).

## 2.4. Objective of the follow-up research

The topic of security is one of the top concerns with regards to CC. Security is often the main “brake” for migrating to a CC model (Bouchaala et al. 2017:303).

The researched literature focusses on general cloud security and deployment of ESA in a SAAS model, and mainly addresses limited topics, such as authentication, authorization and threat/vulnerabilities, and often ignores some other security related issues such as vendor lock-in, jurisdiction/location, operations management and governance. Despite the fragmented picture and the conclusions on the different research sub-questions, the combined content of the various articles provides a justified reason for the continuation of the research.

This follow-up research will give an insight in the use of ESA in a SAAS CC environment with regards to security and risk control, and the deployment of ESA in a SAAS CC service model.



### 3. Methodology

This chapter describes the approach and purpose of the research. In addition, this chapter describes the strategy, method, technique and required resources. Finally, validity, reliability and ethical aspects are discussed.

#### 3.1. Conceptual design: select the research method(s)

Saunders defines five research purposes/studies (Saunders, Lewis, and Thornhill 2019:186–88):

1. Exploratory studies
2. Descriptive studies
3. Explanatory studies
4. Evaluative studies
5. Combined studies

Because it is not yet clear how elements of ESA is used for SAAS CC, the research is exploratory and descriptive in nature. No hypothesis is formulated here. The aim is to find out what actually happens around the use of ESA and risk and security controls, in combination with the SAAS model. As a result of this practical research approach, a clear picture may emerge on basis of which we can address the descriptive part of this research. This study falls into the category of combined studies (Saunders et al. 2019:189–211).

The empirical research had to meet the following selection criteria:

1. The method was used to gain insights in the use of the researched risk and security elements for SAAS CC, and the degree of deployment of ESA in a SAAS CC model
2. The method was suitable for research on the defined elements and to corroborate on the statements made
3. The method could be implemented within six months (duration of the graduation process)

In alignment with above criteria, a concurrent mixed method research was conducted. Concurrent mixed methods research involves the separate use of quantitative and qualitative methods within a single phase of data collection and analysis (Saunders et al. 2019:182). This allows both sets of results to be interpreted together to provide a richer and more comprehensive response to the research question in comparison to the use of a mono method design (Saunders et al. 2019:182). Also, the mixed method may be used in order to combine data to ascertain if the findings from one method mutually corroborate the findings from the other method (Saunders et al. 2019:185).

Given the limited time frame, the outburst of the coronavirus pandemic, and the complex and multi-faced nature of the selected SMEs, an inductive holistic multi-case study research approach was adopted. Such an approach is holistic because it covers one SME as a single entity. The unit of analysis was the SME.

## 3.2. Technical design: elaboration of the method

Because of the usage of mixed methods, this elaboration was done for 2 methods: quantitative method and qualitative method. Both methods are using the same dimensions.

### Dimensions

The eight elements that were deducted from the literature research for RQ1 have been merged into four main groups, called dimensions. A dimension represents the elements that logically can be linked together and can be handled as one subject during survey/interview sessions.

Dimensions for RQ1:

- Compliance and Regulation (RQ1)
- Identification, Authentication and Authorization (RQ1)
- Operational maintenance and Administration (RQ1)
- Architecture (RQ1)

On top of these four dimensions an additional dimension was added for the subject that was deducted from the literature research for RQ2:

- Deployment of ESA in a SAAS service model (RQ2)

### Quantitative method:

The Quantitative research method part is used to gather information through numerical data. Quantitative research examines relationships between variables, which are measured numerically and analyzed using a range of statistical and graphical techniques (Saunders et al. 2019:178). It is used to quantify the opinions.

The use of this method made it easier and faster for respondents to answer by making use of a limited set of pre-defined answers (closed questions). This method also made it easier for the analyst because answers could be quantified (numerical data). Due to the limited number of respondents, this method ensured that more "homogeneous" answers could be obtained, which could therefore be compared across the different cases.

For the quantitative part a survey collected data from a number of resources (Saunders et al. 2019:181). The survey has a pre-determined set of closed questions.

The survey structure is as follows:

The survey took place based on the researched dimensions. For each researched dimension a limited number of closed questions was defined. In addition a score template (Appendix E) was defined to quantify the answers. The numerical score of each question is corrected with a weight indicator to ensure that each dimension is equally valued.

### Qualitative method:

The Qualitative research method part is used to gather non-numerical data. In the qualitative research, meanings are derived from words and images, not numbers. Since words and images may

have multiple meanings as well as unclear meanings, it is often necessary to explore and clarify these with participants. Methods used are unstructured or semi-structured. (Saunders et al. 2019:179). Theme identification is one of the most fundamental tasks in qualitative research (Ryan and Bernard 2003).

For the qualitative part the data collection was done via semi-structured interviews. A semi-structured interview was more appropriate because with an unstructured interview it is difficult to get answers on the specific research questions.

#### **Concurrent mixed method:**

Because of the use of the concurrent mixed method, the data collection (survey and interview) took place at the same time.

Participants in the survey/interview session had to be acquainted with utilization of ESA, SAAS and risk- and security controls within their organization. Together with a manager of the organization a respondent was appointed.

The participants were informed in advance and were able to prepare and plan for the survey/interview session. In this way it was also possible to align with restrictions due to corona pandemic and make optimal use of their limited availability.

Survey/interview execution steps:

1. Introduction
2. Explanation of structure (survey versus interview)
3. Conducting survey/interview: discussion based on survey/interview questionnaire
4. Verification: verification of interview findings with survey score
5. Closure

### 3.3. Data analysis

#### **Quantitative data analysis**

During the survey/interview session, the interview protocol (appendix C) was leading. Survey and interview questions were asked in accordance with the protocol, and the response was noted down for the survey as well as the interview questions. In case a question could not be answered sufficiently, the interviewer tried to elaborate on the question in order to get the necessary information. If the respondent agreed, then the interview was recorded with audio equipment. For each survey/interview a report was created. The report was an accurate interpretation of the information that was collected from the respondent during the survey/interview. The report was sent to the respondent for final verification. During the verification period the respondent could give feedback. Based on the feedback the report was reviewed and adjusted.

The data of the survey was analyzed by using a score template including a scale- and a weight indicator. The scale indicator was setup per question and was based on a Likert-type scale (Saunders et al. 2019:528). In this case it was decided to use a 2-point (no neutral option) and a 3-point (including neutral option) pre-defined scale to avoid a choice overload and because of the fact that selected respondents didn't have extensive information on every researched topic.

The weight indicator was setup per dimension and distributes the weight of the questions in an equal way across the dimension. Survey questions were setup to represent the same level of detail. Therefore, each question has also the same weight within a dimension. The number of questions per dimension may vary. A weight is assigned to each question per dimension, so that the number of questions does not affect the score of a dimension.

Detailed information for the quantitative analysis can be found in Appendix F.

### **Qualitative data analysis**

Our approach for deriving themes during the qualitative research was based on the technique of finding similarities and differences (Ryan and Bernard 2003:91). This technique is used in cases where there is textual data, verbatim text, no rich narrative, and only brief descriptions (Ryan and Bernard 2003:102).

To find similarities and differences in the textual data from the interviews, we used a Natural Language Processing (NLP) method for approximating how similar two texts are: cosine similarity (Tan, Steinbach, and Kumar 2005:500).

NLP refers to the branch of computer science concerned with giving computers the ability to understand text and spoken words in much the same way human beings can. In NLP the calculations are performed on numeric representations (vectors) of text objects.

Cosine similarity is a widely implemented metric in information retrieval and related studies. This metric models a text as a vector of terms and the similarity between two texts is derived from cosine value between two texts' term vectors (Rahutomo, Kitasuka, and Aritsugi 2012).

To compute the cosine similarity between interview responses we used functions provided by the spaCy NLP library. spaCy is a free open-source library for Natural Language Processing in the Python programming language. spaCy provides languages models (learned from large collections of text) to find semantic related words or sentences in text.

We have written a Python program that reads an excel file with the interview answers of all respondents, calculates the similarity of the answers and adds the results of the calculations to the excel file.

Since cosine similarity can only be calculated for two vectors, we calculated the similarity between the respondents' answers for each question in pairs. This resulted in 3 pairs of similarity calculation: interview 1/2, interview 1/3 and interview 2/3, represented in the analysis excel file by the three columns Spacy12, Spacy13 and Spacy23.

When the calculated cosine similarity is greater than 0.66, the spreadsheet cell is colored green, indicating that we have a high degree of similarity. When the calculated cosine similarity is less than 0.33, the spreadsheet cell is colored red, indicating that similarity is low. If the calculated cosine similarity is between 0.33 and 0.66, the spreadsheet cell will be colored yellow, indicating that there is some similarity.

In the analysis excel file the column similarities/differences represents the degree of similarity/difference as a final result. In case of one or more red colored spaCy columns the similarities/differences column will be colored red to indicate a difference. In case of a combination of green and yellow spaCy columns, the similarities/differences column will be colored green to indicate a similarity. In case of only yellow spaCy columns, the similarities/differences column will be colored white to indicate a low similarity.

In the following Figure you will find an extract of the python code used for processing the spaCy library.

```
# Load large Dutch language model of spaCy and assign the model to the variable "nlp_nl":  
nlp_nl = spacy.load('nl_core_news_lg')  
# Process sentences A and B with the language model to convert the sentences to vectors:  
vector_A = nlp_nl(sentence_A)  
vector_B = nlp_nl(sentence_B)  
# Compute the cosine similarity for vectors A and B:  
similarity = vector_A.similarity(vector_B)
```

Figure 3 Extract of Python code using the spaCy library

Looking at the degree of similarity, we can formulate and appoint themes that are important (or appear to be completely unimportant) for all respondents.

Detailed information for the qualitative analysis can be found in Appendix F.

### 3.4. Reflection w.r.t. validity, reliability and ethical aspects

#### Internal validity

Internal validity refers to the extent that findings can be attributed to the intervention that is researched rather than to flaws in the research design: does the research actually investigate what is intended to be investigated (Saunders et al. 2019:215).

Data is collected and analyzed through survey and interviews in order to come to the final results. In this context, the following actions are taken:

- A test interview was held to check if the setup of the combined method (survey and semi-structured interview) was comprehensible, and to confirm that the right questions were being asked.
- To prevent the respondents from saying less than they would like it is pledged that the results are anonymous. Only roles (function title) are mentioned in the reports.
- At the time of scheduling the interviews, the purpose of the research is explained and background information is provided. In this way respondents are informed in advance and they have the opportunity to prepare for the interview.
- All respondents had similar relevant experience in the researched area.

#### External validity

The external validity is concerned with the question if the research findings can be generalized to other contexts (Saunders et al. 2019:216). As this research is conducted within a small number of organizations it will have a limited score on external validity.

By describing the research in terms of context, design and outcomes, it is possible to assess the research and increase external validity (Saunders et al. 2019:5.8).

## **Construct validity**

Construct validity refers to the extent to which a set of questions actually measures the presence of the construct you intended them to measure (Saunders et al. 2019:517).

Measures taken to maximize construct validity:

- Survey/interview is conducted within the case organization on basis of a predefined protocol for surveying/interviewing.
- Respondents receive information in advance to prepare for the survey/interview
- Data that is collected through survey/interview is clustered per research dimension
- after creating the survey/interview report with results, the respondent is given a period of time to give feedback on the survey/interview results and the interpretation of the researcher.
- All steps as described above will be documented in the report.
- The chosen research method could be validated based on the findings of the respondents (do respondents confirm that the chosen method is a valid method for collecting data within the organization, do the results obtained reflect the situation within the organization).

## **Reliability**

In the context of reliability, it is important that the research must be replicable by other researchers (Saunders et al. 2019:213). The following measures are taken to enable replication of the study:

- The data that is retrieved from the survey and interview is obtained with the consent of the respondent and summarized in the interview reports. After receiving the report, the respondent is given a period of time to provide feedback. This feedback may result in adjustment of the report.
- During this research we consulted different persons for collection of relevant data.
- Respondents from different companies are interviewed individually to ensure that company information stays anonymous.

## **Ethical aspects:**

Following measures were applied to safeguard research ethics (Saunders et al. 2019:6.6):

- The respondents voluntarily participate in the interview.
- The respondents are informed that they are not obliged to answer.
- The data used and processed cannot be traced back to the respondents.
- The data used and processed cannot be traced back to the organization.
- During the research, we work in accordance with the “wet bescherming persoonsgegevens (AVG)” and the Dutch Code of Conduct for Scientific Practice.

## **Limitations:**

The research certainly also has some limitations:

- To validate the findings on a larger scale, the research could be further expanded and broadened with additional associated risk and security elements.

- The survey would also be more reliable with a higher number of respondents and representation from several different departments and even more companies, not only being SMEs.

## 4. Results

This section describes the implementation of the research and discusses the outcome obtained through the research. The scores are linked to the outcome of the survey questions (Appendix E). The results are linked to the different themes (T1/T31) that have been extracted from the qualitative data analysis phase (Appendix F). Per theme the number of occurrences was registered to indicate the “importance” of a theme (Appendix G). Themes that have four or more occurrences are marked in green color.

### 4.1. Case organizations

Because of unplanned circumstances (corona pandemic) only a limited number of case organizations (three) and related respondents (three) could be identified. An overview of participating case organizations can be found in appendix A. An overview of respondents can be found in appendix B. The selection of respondents is aligned with management of the case organization and is based on objective criteria, such as the knowledge of information technology in general and the knowledge in the area of ESA, SAAS and risk- and security controls within their organization.

All three case organizations are SME organizations (T1). All respondents have a clear understanding of the definitions for ESA, CC and SAAS (T2). For all case organizations the goals for ESA are formalized (T3). All organizations had core business applications that were delivered via the SAAS service model (T6, T15) and different risk and security controls were implemented (T7).

### 4.2. Implementation of the research

#### 4.2.1. Surveys

Data collection has partly been conducted by using closed questions survey. Due to the corona pandemic and strict regulations all surveys were executed online via Microsoft Teams. Each survey session was planned for 1 hour (combined with interview questions).

The best possible survey score that a respondent could achieve for each dimension was 100%. A score of 100% indicates that maturity of the selected dimension in terms of minimizing SAAS related risk and security problems is very high. The lowest possible score that a respondent could achieve for each dimension was 0%. A score of 0% indicates that maturity of the selected dimension in terms of minimizing SAAS related risk and security problems is very low.



## 4.2.2. Interviews

Data collection has partly been conducted by using semi-structured interviews. Due to the corona pandemic and strict regulations all interviews were executed online via Microsoft Teams. Each interview session was planned for 1 hour (combined with survey questions).

## 4.3. Results

In this section the results of the survey and semi-structured interviews are presented. This section will also provide evidence on the main research question and the sub-questions.

The following sub-sections are structured according to the different dimensions that were deducted from the key elements (RQ1), and one additional dimension for the subject of deployment of ESA in a SAAS service model (RQ2).

### 4.3.1. Compliance and Regulation

In this section the score and results for the dimension compliance and regulation are presented. The score is presented in a table. In the table you will find the individual (total) scores as well as the combined (total) scores for the surveyed dimension. In addition, you will find the results from the semi-structured interviews.

Score:

Nr.	Vraag (NL)	Question (EN)	Score RESPONDENT1	Score RESPONDENT2	Score RESPONDENT3	Score TOTAL
1.1	Voldoet de SAAS-oplossing(en) aan geldende wet- en regelgeving?	Does the SAAS solution(s) comply with applicable laws and regulations?	50%	50%	100%	66,7%
1.2	Worden gegevens in de SAAS applicatie(s) uitsluitend gebruikt of verwerkt in overeenstemming met het oorspronkelijke beoogde doel?	Is data in the SAAS application(s) used or processed solely in accordance with the original intended purpose?	100%	100%	100%	100%
1.3	Is de toegang tot gegevens en de opslag van gegevens beveiligd middels voorgeschreven encryptie methoden?	Is access to data and data storage secured by prescribed encryption methods?	50%	100%	50%	66,7%
1	De SAAS oplossing voldoet aan compliance en regelgeving	The SAAS solution complies with compliance and regulations	66,7%	83,3%	83,3%	77,8%

Table 2 Compliance and Regulation score

Result:

Legal and regulatory compliance was one of the priority issues for all case organizations when it came to security and risk of data access and storage in SAAS applications (T7). Legal and regulatory requirements and standards in different geographic regions/jurisdictions require data to be

physically stored in a designated country/legal jurisdiction. For all respondents there is a high confidence that SAAS application comply with legal and regulatory requirements. Especially for the case organization that operated in healthcare area there were more strict requirements for access and data storage (T9) of medical information, but also here confidence was high. All case organizations (healthcare, accountancy, governmental) were subject to periodic audits (T10) and relied on the compliance information from the certified SAAS CSP (T11). All case organizations indicate that they are processing sensitive data (personal, financial, medical) which becomes a big problem when data is leaked (T5).

All respondents confirmed that the data in the SAAS application is solely used in accordance with the original intended purpose (T12). In all case organizations the intended purpose was identified by management and written down in strategy documents (T3). This was needed to be in line with legal regulations.

Access to data and data storage via encrypted methods was implemented for each case organization. But there was only a full coverage of encryption for one case organization. In case encryption is not secured sensitive data can be leaked (T5).

### 4.3.2. Identification, Authentication and Authorization

In this section the score and results for the dimension identification, authentication and authorization are presented. The score is presented in a table. In the table you will find the individual (total) scores as well as the combined (total) scores for the surveyed dimension. In addition, you will find the results from the semi-structured interviews.

Score:

Nr.	Vraag (NL)	Question (EN)	Score RESPONDENT1	Score RESPONDENT2	Score RESPONDENT3	Score TOTAL
2.1	Moeten gebruikers van de SAAS-applicatie(s) zich authenticeren?	Should users of the SAAS application(s) authenticate themselves?	100%	100%	100%	100%
2.2	Kan de SAAS-applicatie(s) de identiteit van de gebruiker vaststellen?	Can the SAAS application(s) determine the identity of the user?	50%	50%	50%	50%
2.3	Is er een beleid voor toegang en gebruikscntrole?	Is there an access and usage control policy?	100%	100%	100%	100%
2	De SAAS oplossing voldoet aan identificatie, authenticatie en autorisatie vereisten	The SAAS solution meets identification, authentication and authorization requirements	83,3%	83,3%	83,3%	83,3%

Table 3 Identification, Authentication and Authorization score

Result:

For all case organizations the way of electronic authentication of humans in a SAAS application was a problem (T13) and caused issues in the area of balancing between usability and security. All organizations used a combination of the traditional three factors:

- something the user knows (user-id / secret password),
- something the user has (physical possession) and
- something that is a unique trait of the user (biometrics, for example smartphone fingerprint)

The combination of all three factors provided a high level of security. In one organization for certain cases only the first factor (user-id/password) was used for authenticate with the a SAAS application. In most cases 2FA authentication was used in combination with a smartphone to access the SAAS application. All case organizations did use a registration policy (T14).

Two case organizations confirmed that there were cases in which the identity could not be confirmed. In case authentication or identification is not secured this can lead to a sensitive data leak (T5).

All of the case organizations had a policy and guidelines (T4) for access and usage of SAAS applications. The policy and guidelines were aligned with the configuration of the SAAS applications. In case of authorization (user permissions) failure, sensitive data can be leaked (T5).

### 4.3.3. Operational maintenance and Administration

In this section the score and results for the dimension operational maintenance and administration are presented. The score is presented in a table. In the table you will find the individual (total) scores as well as the combined (total) scores for the surveyed dimension. In addition, you will find the results from the semi-structured interviews.

Score:

Nr.	Vraag (NL)	Question (EN)	Score RESPONDENT1	Score RESPONDENT2	Score RESPONDENT3	Score TOTAL
3.1	Wordt de beschikbaarheid van de SAAS-applicatie(s) gegarandeerd?	Is the availability of the SAAS application(s) guaranteed?	50%	50%	100%	66,7%
3.2	Worden kwetsbaarheden in de SAAS-applicatie(s) gedetecteerd?	Are vulnerabilities detected in the SAAS application(s)?	n.a.	n.a.	100%	n.a.
3.3	Wordt er gebruik gemaakt van SLAs die ook security elementen bevatten?	Are there SLAs used that also include security elements?	n.a.	n.a.	100%	n.a.
3	Operationeel beheer en administratie voldoet aan vereisten	Operational management and administration meet requirements	50%	50%	100%	66,7%

Table 4 Operational maintenance and Administration score

In two cases we deleted two questions in our results (marked with n.a.) because the respondents were unable to answer the questions. As a result, the score might not give a correct indication of the average level of this dimension for the three case organizations.

Result:

Availability of SAAS applications was a crucial aspect for all case organizations (T15, T16). For two case organization there was a max score on guaranteeing SAAS availability, for one case organization this was limited to a certain amount of up-time (T27, T30).

Within two case organizations it was not clear if there was any ability of detection of vulnerabilities that could impact SAAS applications (T17). In another case organization this was completely covered. In case vulnerabilities are not detected and repaired there is a risk for leakage of sensitive data (T5).

In one case organization SLAs were used that also included security elements like uptime, vulnerability and threat monitoring. The other case organizations could not answer the question about security elements in the SLAs (T19). One respondent said that within his organization *“it is not clear whether SLAs also include security elements”*.

Detected vulnerabilities are not immediately reported to the SAAS customer (T31). This can lead to unexpected leakage of sensitive data (T5). Customers also doubt whether providers inform them on short term about detected vulnerabilities or leaks (T18).

Server fail-over is available for most SAAS applications (T16) .

#### 4.3.4. Architecture

In this section the score and results for the dimension architecture is presented. The score is presented in a table. In the table you will find the individual (total) scores as well as the combined (total) scores for the surveyed dimension. In addition, you will find the results from the semi-structured interviews.

Score:

Nr.	Vraag (NL)	Question (EN)	Score RESPONDENT1	Score RESPONDENT2	Score RESPONDENT3	Score TOTAL
4.1	Heeft u een beeld van de architectuur van de SAAS-applicatie(s)?	Do you have a “picture” of the architecture of the SAAS application(s)?	50%	0%	50%	33,3%
4.2	Bezit de CSP certificaten voor de SAAS applicaties?	Does the CSP hold certificates for the SAAS applications?	50%	50%	100%	66,7%
4.3	Wordt de SAAS applicatie benaderd via beveiligingsprotocollen?	Is the SAAS application accessed via security protocols?	100%	100%	100%	100%
4	Architectuur is inzichtelijk	Architecture has clear insights	66,7%	50%	83,3%	66,7%

Table 5 Architecture score

Result:

In all case organizations there only was a limited picture of architecture of the SAAS applications (T20). In two case organizations this was limited to a high-level overview of infrastructure and applications. In one case organization there was no insight at all. One respondent mentioned that *“within a SAAS model the security architecture is handled by the provider of the application”*.

In all case organizations the CSP used certificates, but in two case organizations it was not clear what kind of certificates were used (T22, T28). In one of the case organizations the “PKI overheids-certificaten” were used. These certificates are compliant with specific governmental

requirements and are mandatory for securing electronic services within and between the SAAS applications of government institutions and other parties.

In all case organizations security protocols were used for accessing SAAS applications (T23). Protocols used were encrypted (https) and using SSL certificates.

In all case organization there are also possibility to access SAAS applications via API interfaces (T21). In case unauthorized devices are able to access the SAAS application there is a high risk of leaking sensitive data (T5).

### 4.3.5. Deployment of ESA in a SAAS service model

In this section the score and results for the dimension deployment of ESA in a SAAS service model is presented. The score is presented in a table. In the table you will find the individual (total) scores as well as the combined (total) scores for the surveyed dimension. In addition, you will find the results from the semi-structured interviews.

Score:

Nr.	Vraag (NL)	Question (EN)	Score RESPONDENT1	Score RESPONDENT2	Score RESPONDENT3	Score TOTAL
5.1	Gebruikt u ESA om de risico's van SAAS in kaart te brengen/te beheren?	Are you using ESA to identify/manage the risks of SAAS?	50%	0%	50%	33,3%
5.2	Is er een budget voor risicobeheer en monitoring van SAAS applicaties?	Is there a budget for risk management and monitoring of SAAS applications?	50%	50%	50%	50%
5.	Risico's worden middels ESA in kaart gebracht en beheerd	Risks are mapped and managed through ESA	50%	25%	50%	41,7%

Table 6 Use of ESA in a SAAS service model score

Result:

All respondents confirmed that elements of ESA were used within their case organizations to identify and manage risks for SAAS applications (T8, T29). The usage was based on ad-hoc requirements from management and/or from regulation/compliance point of view. In all researched organizations there was no roadmap for ESA. Also, there was only a limited use (T8) of SAAS related service portfolio (T24, T25, T26). One respondent stated that *“there is no usage of a service portfolio with regards to risk and security for SAAS at all”*.

All respondents confirmed that there was a limited budget for risk management and monitoring of applications, including SAAS (T26, T1, T24). None of the respondents could give an indication on the percentage of the budget that was dedicated for SAAS. For all three case organizations there was no ESA related governance setup for SAAS (T24, T29, T1). One respondent mentioned that *“there is no specific role or function that is dedicated for monitoring of SAAS applications within our SME organization, this work is done as part of a regular job profile”*.

## 5. Discussion, conclusions and recommendations

This chapter contains a discussion of the outcomes. What do the results mean, what is the position of these results in relation to the literature and what is it we have actually learned from the results.

### 5.1. Discussion – reflection and limitations

#### 5.1.1. Discussion - reflection

Using the survey and interview results we can discuss and reflect the implications for the dimensions defined in chapter four: what is the position of these scores and results in relation to the literature and what is it we have actually learned. Reflections are linked to the most important themes as identified in Appendix G.

The following figure gives an overview of the combined scores per dimension. These scores are discussed in the next sections.

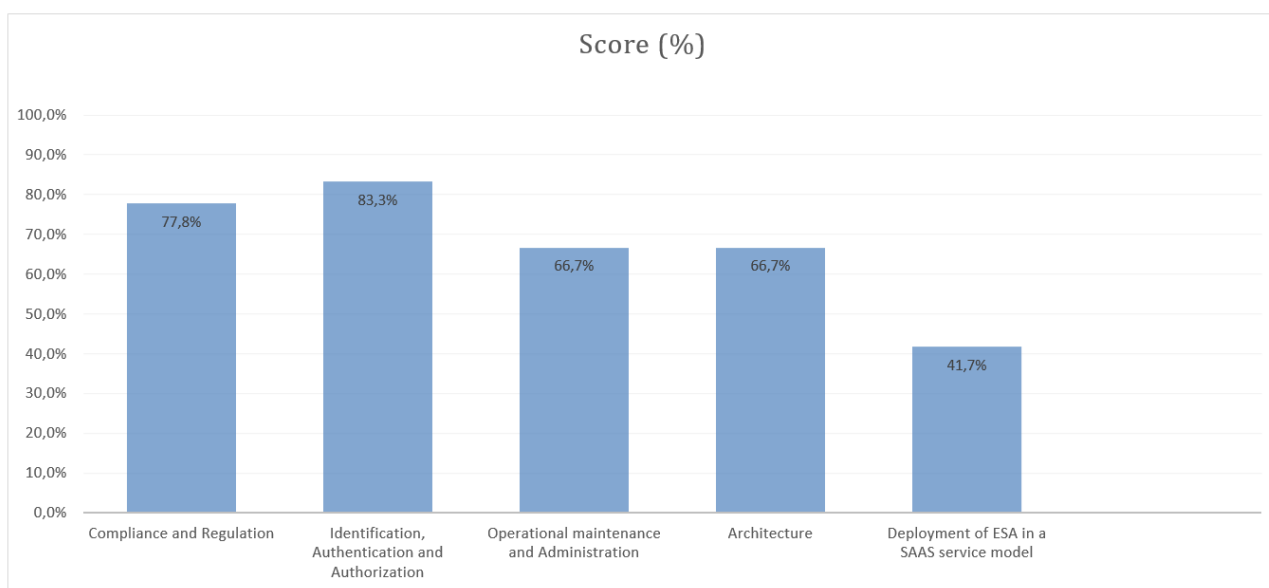


Figure 4 Overview of combined score per dimension

### Compliance and Regulation

The respondents are confident that the SAAS solution complies with compliance and regulations (high total survey score 77,8% (figure 4), positive interview answers). The SAAS providers provide their customers (extensively or not) with information about annual audits and possible certifications, with which they try to demonstrate their compliance. Encryption is used by all SAAS providers, especially for transport/communication of data and usually also for the storage of data. The data in the SAAS application is in all cases solely used in accordance with the original intended purpose. SAAS users however rely largely on the information provided by the SAAS providers to fund their statements about compliance of the SAAS applications. The SAAS users themselves are subjected to

an annual audit of the organization, although this audit may focus more on the user organization and its local applications and less on the use of SAAS applications.

The adoption of SAAS has some barriers, and one of these is issues regarding compliance, privacy and legal matters (Hashizume et al. 2013). One of the top-level cloud security requirements is that the SAAS application must ensure regulatory compliance (Rath et al. 2019).

Results show that SMEs do not hesitate in using SAAS applications, as they rely on the compliance information from the SAAS providers and the successful audits. This can be related to the finding that the importance of trust in the cloud computing context has been repeatedly highlighted due to the lack of transparency surrounding cloud offerings, and customers' inability to fully audit cloud services (van der Werff, Fox, Masevic, Emeakaroha, Morrison, and Lynn 2019).

(This can be linked to theme T1, T5, T11).

## Identification, Authentication and Authorization

The respondents are confident that the SAAS solution meets identification, authentication and authorization requirements (high total survey score 83,3% (figure 4), positive interview answers). Users of the SAAS application(s) have to authenticate themselves. Most SAAS applications use 2FA for identification and authentication, but there are also SAAS applications that can be accessed with only login name and password. All of the case organizations have a policy and guidelines for access and usage (authorization) of SAAS applications. However, two case organizations report that there are SAAS applications in which the user identity cannot be confirmed. Some SAAS applications that are only used with login name and password (no use of 2FA) are vulnerable for hacking and phishing. The authentication method is the main factor of preserving security and privacy of each communication in cloud computing (Purohit and Rana 2016). If authentication and identification is not secure, the SAAS user may have problems when data (medical, financial data) is leaked. This can lead to fines by the Dutch Data Protection Authority and the AFM. In addition, SAAS users very often process data of their own customers in the SAAS application. These customers may be able to claim damages if their data are leaked.

As a best practice, any of the multifactor authentication mechanism in association with the traditional credential-based authentication must be used (Indu, Anand, and Bhaskar 2018).

Yubico research reveals more than three quarters of enterprises in the UK, France and Germany are undervaluing Two-Factor Authentication. The research was conducted with 3,006 employees at large organizations (250+ employees), who have worked from home at some stage and have work issued devices in the UK, France and Germany between February 19, 2021 and March 3, 2021.

(Yubico 2021)

The results show that there are policy and guidelines for most of the SAAS applications and that they are accessed with a multifactor (2FA) authentication mechanism, but there are some exceptions.

The fact that 2FA in some cases is not used is confirmed by recent research: despite 2FA technology being the best line of defense to protect against account takeovers, only 22% of respondents report their company has introduced it since the pandemic began (Yubico 2021). Furthermore, results show that authentication and identification are also not always secured enough. This is also in alignment with the findings that SAAS providers need to ensure the security and privacy in order to overcome threats such as broken authentication since the huge amount of personal and sensitive data will be moved to the cloud platform (Subashini and Kavitha 2011).

(This can be linked to theme T4, T5, T13).

## Operational maintenance and Administration

The respondents have only limited confidence that SAAS solutions meet the requirements of operational maintenance and administration (medium total survey score 66,7% (figure 4), neutral interview answers).

However in our results two questions were removed, because the respondents were unable to answer the questions. As a result, the total score does not give a good indication of the average level of operational maintenance in the three case organizations.

The availability of the SAAS applications is guaranteed, but in some cases not to the maximum. In some cases, there is only limited operational uptime. This may lead to failure of core activities. This is a key topic within healthcare industry. CSPs have diversion options to other server locations. This is also stated in SLAs. SAAS Customers are doubting whether providers inform them directly about detected vulnerabilities or leaks in an application (news reports show that CSPs usually only disclose leaks after some time). In the Netherlands you must report a data breach to the Dutch Data Protection Authority within 72 hours of discovery of the leak. But if no privacy relevant data is lost, there is no obligation to report the security incident to the authorities or to the SAAS customers (Autoriteit Persoonsgegevens Groep gegevensbescherming artikel 29 2018).

Denial-of-service is the common attack in cloud and maintaining availability of the cloud services in the face of distributed denial-of-service attacks is important to ensure proper service for users (Rath et al. 2019). Since cloud services are delivered using classical network protocols and formats over the Internet, implicit vulnerabilities existing in these protocols, as well as threats introduced by newer architectures, raise many security and privacy concerns (Modi et al. 2013). The number of security vulnerabilities in the cloud is more than in traditional enterprise services (Niu et al. 2016). In today's complex Cloud systems, with multiple endpoints and edge nodes, makes manual daily systems administration and security monitoring and analysis difficult if not entirely impossible (Rath et al. 2019).

Results show that respondents have confidence in the availability of the SAAS application, but have no up to date insights in the amount and severity of security vulnerabilities and threats of the SAAS application. They completely rely on the CSP for operational maintenance and administration. Therefor SAAS vendors should guarantee security, availability and performance through clear SLA in which a common understanding about service, priorities, responsibilities and guarantees between service provider and client is determined (Safari, Safari, and Hasanzadeh 2015). (This can be linked to theme T11, T15, T31).

## Architecture

The respondents have only limited confidence that SAAS solutions meet the architectural requirements for security (medium total survey score 66,7% (figure 4), neutral interview answers). All case organizations have a limited view of the architecture of the SAAS applications (not all providers inform their customers extensively about the technical and logical security related infrastructure and systems). The providers do have certificates, such as ISO 27001. The SAAS applications are all accessed by encrypted protocols (https) using SSL certificates, which is also clearly stated in the SLAs. Vendors and developers must consider key architecture factors for SAAS development process to stand in the current competitive environment: these key factors include customization, scalability, MTA (Multi-Tenancy Architecture), security, integration, and fault tolerance and recovery management (Aleem, Ahmed, Batool, and Khattak 2019).



Results show that the SAAS CSC have no insights in the technical and logical security architecture of the SAAS application. Insights in SAAS architecture are limited to encryption and security protocols for accessing the SAAS application. This is in line with findings that customers typically are unaware of the network behind a SAAS-solution, as they only deal with the SAAS-provider. The customer pays the SAAS provider who in turn pays the different parties involved to deliver its service (Van Velzen, De Jong, and Jansen 2019:8). The availability of SAAS applications relies on the robustness of the SAAS-provider and its underlying parties. With every additional party there are more places the network could “break”, increasing the chance of business interruption (Van Velzen et al. 2019:9). (This can be linked to theme T20).

### *Deployment of ESA in a SAAS service model*

The respondents have only limited confidence that the SAAS risks and security controls are mapped and managed through ESA (low total score 41,7% (figure 4), neutral interview answers).

ESA is used to a very limited extent in all organizations to identify the risks and security controls of SAAS. The use of ESA-related functions within the organizations is limited to the deployment of a data management officer (probably motivated by the legal obligation under the GDPR). Other functions/roles are carried out jointly to a limited extent by an ICT administrator/manager (from the point of view of cost savings/low budget). There is no ESA related governance. A limited budget is available for risk and security management. There are no specific ESA functions/roles with regards to SAAS. Within an SME a system administrator does this work periodically.

A key part of defining the enterprise architecture team is establishing the expected role and mandate of the security architect. Best practice security architecture integrates security and risk within all domains. Integral to this is establishing the governance process for the security architecture within the context of the enterprise architecture governance process (The open group 2016).

From the results it is recognized that in none of the researched case organizations there is a typical governance setup, nor a dedicated security architect with regards to ESA in a SAAS service model. There is only a limited budget available for security and risk issues. The major risk in risk management is that a risk occurs and there is not enough time in the schedule or money in the budget (Westcott 2005).

(This can be linked to theme T8, T24, T26, T29).

### 5.1.2. Discussion - limitations

Because of the coronavirus outbreak the initial case organization had to cancel participation in the research at the last minute. During a new search for a case organization, three SME case organization could be identified for participation in the research. This resulted in change from a single-case study to a multi-case study approach, and several adjustments in research setup had to be made. Because of this also a smaller number of respondents was interviewed than originally anticipated, which could lead to less substantiated data. The timeframe for arranging and executing the data collection, and the data analysis was squeezed and became even more time critical.

For data collection a mixed method was used. This mixed method consists of two parts. Part 1 (quantitative): a survey approach for the main questions. For this a score template was developed in

order to be able to collect a score per main question. Part 2 (qualitative): a semi-structured interview approach with open questions to corroborate the related survey questions. The open detail questions should substantiate and underpin the score of the main question.

Another issue was finding a suitable data analysis technique for the qualitative part. Due to the smaller number of respondents (three) the usage of thematic analysis was not recommended. A minimum of four respondents is required to make this technique efficient (Ose 2016). Another disadvantage of thematic analysis is that although there are numerous examples of how to conduct qualitative research, there are few discussions in the literature about how to conduct a rigorous and relevant thematic analysis (Nowell, Norris, White, and Moules 2017). While thematic analysis is flexible, this flexibility can lead to inconsistency and a lack of coherence when developing themes derived from the research data (Holloway and Todres 2003). There is no clear agreement about how researchers can rigorously apply this method (Nowell et al. 2017).

Thematic analysis seems to be almost equivalent to labeling/coding and categorizing by theme in the literature, but there are many techniques for finding themes (Ryan and Bernard 2003). Since the textual data consisted of brief descriptions a different technique, based on finding similarities and differences, was used (Ryan and Bernard 2003:102). This technique was supported by an NLP engine and made use of an open-source library (Spacy 2021) for advanced NLP (Weiyang, Pham, Eftekharypour, and Pheng 2019).

The research setup of this thesis concerned a multi-case study approach. But with the limited number of respondents, the most prominent critique factor for this analysis is the issue of external validity or generalizability: because of the limited number, the findings cannot be widely accepted.

Due to restrictions in timing, the literature study was not exhaustive. Because of this an incomplete picture of the investigation of the research topic may occur.

This research has been executed during the challenging time of the corona pandemic. Because of this, participant bias could occur. People may behave differently during an interview (McCambridge, Witton, and Elbourne 2014). All meetings were executed via Microsoft Teams (online). This also makes it more difficult to exclude participant's bias.

## 5.2. Conclusions

SAAS allows users to connect to and use cloud-based applications over the Internet. The use of SAAS applications continues to grow, making companies more and more dependent on the SAAS CC service model in the future. In this thesis we researched to what extent Enterprise Security Architecture (ESA) can be used to map/model risk and security controls in a SAAS CC service model (RQ).

To be able to answer this main research question we first had to investigate and answer two sub research questions: sub-research Question 1 (RQ1): What is the impact of using the SAAS CC service model on risk and security controls and sub-research Question 2 (RQ2): How is ESA being deployed in a SAAS CC service model.

Results from literature research showed that there is only very limited knowledge on the actual use of ESA within organizations.

After conducting a survey/interview session within the selected case organizations, we found that the use of SAAS applications can create risks in a number of areas. SAAS applications may have compliance uncertainties, security issues or infrastructure flaws that enable unauthorized access to sensitive customer data.

Below table shows per dimension the impact of the use of the SAAS service model on the risk and security controls (RQ1) and the implications thereof for the use of ESA by the SAAS customer (RQ), based on the discussion of the researched data (bottom-up approach).



	<b>Compliance and Regulation</b>	<b>Identification, Authentication and Authorization</b>	<b>Operational maintenance and Administration</b>	<b>Architecture</b>
<b>To what extent can ESA be used to map/model risk and security controls in a SAAS CC service model (RQ)</b>  	<p>ESA can be used to identify the risk associated with applications compliance failure</p> <p>The controls to manage the risk, can be partly implemented by the SAAS CSC</p> <p>Compliance and regulation can be controlled and monitored by ESA artifacts like agreements</p>	<p>ESA can be used to identify the risk associated with applications being vulnerable for threats</p> <p>The controls to manage the risk, can be partly implemented by the SAAS CSC</p> <p>Identification, authentication and authorization can be controlled and monitored by ESA artifacts like agreements and user access list</p>	<p>ESA can be used to identify the risk associated with the slow response to threats</p> <p>The controls to manage the risk, cannot be implemented by the SAAS CSC</p> <p>This is the responsibility of the SAAS CSP</p>	<p>ESA can be used to identify the risk associated with the limited view of possible vulnerabilities of the security architecture</p> <p>The controls to manage the risk, cannot be implemented by the SAAS CSC</p> <p>This is the responsibility of the SAAS CSP</p>
<b>Impact on risk and security controls (RQ1)</b>  	SAAS application is not monitored for compliance with regulation	SAAS application vulnerable for threats	The SAAS user cannot respond quickly to threats	Limited view of possible vulnerabilities in the security architecture of SAAS application
<b>Discussion of the research data</b>	SAAS customer trust in SAAS provider compliance information is high	Authentication and identification methods are not secure enough for some SAAS applications	No up-to-date insights in security vulnerabilities and threats	Limited insight in technical and logical security architecture

Table 7 SAAS service model impact and use of ESA

Below table shows how ESA is generally deployed by the customer (RQ2) and the implications thereof for the use of ESA by the customer in a SAAS service model (RQ), based on the discussion of the researched data (bottom-up approach).



	<b>Deployment of ESA in a SAAS service model</b>	
	<b>Budget for risk management</b>	<b>ESA governance setup</b>
<b>To what extent can ESA be used to map/model risk and security controls in a SAAS CC service model (RQ)</b> 	A small budget and limited involvement of resources prevent extensive deployment of (elements of) ESA in general and therefore also specifically for a SAAS CC service model	The limited use of (elements of) ESA complicates the use of ESA for risk and security controls in a SAAS CC service model. This also limits setup of roles and responsibilities to manage ESA related artifacts
<b>How is ESA being deployed (RQ2)</b> 	Limited resources and capabilities involved in risk and security management	(Elements of) ESA is used to a very limited extent by the CSC
<b>Discussion of research data</b>	Limited budget available for risk and security management	No typical governance setup, no dedicated security architect appointed No management involvement

Table 8 SAAS service model ESA deployment

Customers should use ESA to identify the risks of utilizing the SAAS service model and define the controls to manage the risks:

- Trust of the SAAS customer in the compliance of the SAAS provider is high. But actual results show that no (elements of) ESA are in place to check and confirm this trust. The CSC can use ESA tools and methods to guarantee and monitor compliance with regulation.
- Although SAAS customers have a big confidence, the authentication and identification methods are not always secure enough. This could have a big impact on risk and security controls of the SAAS applications. The elements of identification, authentication and authorization can be setup and monitored with ESA.
- SAAS customers have no up-to-date insights in the amount and severity of security vulnerabilities and threats detected in the operational maintenance of the SAAS application. They completely rely on the CSP. ESA can't be used by the CSC to implement the controls needed to manage the risks. These controls are the responsibility of the SAAS CSP.
- The SAAS customer has no insights in the technical and logical architecture of the SAAS application. When SAAS users have no insight in the architecture, they cannot gain insight in the possible vulnerabilities of the SAAS application. The CSC can't use ESA to implement the controls needed to manage the security. These controls are the responsibility of the SAAS CSP.
- ESA is deployed to a limited extent by the CSC. In none of the researched customer organizations there is a typical governance setup nor a dedicated security architect with

regards to ESA. A small CSC budget for risk management and the limited use of ESA in general by the CSC prevents extensive deployment of ESA for a SAAS CC service model.

Both the CSP and the CSC possess responsibility in securing the cloud and minimizing the risk. Shared responsibility does not mean less responsibility. Within a SAAS service model the CSP will cover many aspects of physical, infrastructure, and application security while the CSC remains responsible for certain areas of security and control like compliance, user access and data. The CSC can use ESA to manage the areas of security and control for which he remains responsible, although the current limited use of ESA provides a poor basis for managing the risks of the SAAS CC service model.

### 5.3. Recommendations for practice

It is recommended to create awareness in an SME in the area of risk and security when using SAAS applications.

Within an SME currently there often is limited budget and capacity. This leads to a gap with regards to implementing ESA or elements of ESA in general and specifically for SAAS. It is recommended to plan for budget and capacity with regards to ESA related activities.

It is recommended to have one Single Point of Contact within the CSC for risk and security issues, including SAAS.

Management buy-in and management approval for ESA or elements of ESA is key and recommended.

When using (elements of) ESA, it is recommended to install monitoring artifacts in such a way that ESA continues to be updated and improved.

### 5.4. Recommendations for further research

This research was exploratory and performed in three different SME case organizations within three different industry types (healthcare, accountancy, governmental). Despite the fact that it was executed as a multi-case research, it still has limited generalizability, providing opportunities for subsequent research.

From conclusions it is recognized that there is a shared responsibility between CSP and CSC. But it is not clear for the CSC what his responsibility is. This seems to be a common problem as also stated by a survey of Palo Alto Networks. The state of Cloud Native Security based on a survey of 3,000 professionals in cloud architecture, shows that 73% of organizations report being unsure about where their CSP responsibility for securing cloud workloads stops and where theirs begins (Palo alto networks 2020). This is also providing opportunities for subsequent research.

## References

- Ahlemann, Frederik, Eric Stettiner, Marcus Messerschmidt, and Christine Legner. 2012. *Strategic Enterprise Architecture Management: Challenges, Best Practices and Future Developments*.
- Alam, Shaz, Mohd Mueem, and Suhel Ahmad Khan. 2018. "Review on Security Aspects for Cloud Architecture." *International Journal of Electrical and Computer Engineering (IJECE)* 8(5):3129. doi: 10.11591/ijece.v8i5.pp3129-3139.
- Aleem, Saiqa, Faheem Ahmed, Rabia Batool, and Asad Khattak. 2019. "Empirical Investigation of Key Factors for SaaS Architecture Dimension." *IEEE Transactions on Cloud Computing* 1–1. doi: 10.1109/TCC.2019.2906299.
- Autoriteit Persoonsgegevens Groep gegevensbescherming artikel 29. 2018. *Richtsnoeren Voor de Melding van Inbreuken in Verband Met Persoonsgegevens Krachtens Verordening 2016/679*.
- Bouchaala, Mariem, Cherif Ghazel, Leila Azouz Saidane, and Farouk Kamoun. 2017. "End to End Cloud Computing Architecture Based on A Novel Classification of Security Issues." Pp. 303–10 in *2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA)*. Vols. 2017-Octob. IEEE.
- Caballero, Albert. 2020. "Advanced Security Architecture for Cloud Computing." *Cloud Computing Security: Foundations and Challenges* 443.
- Gonzalez, Nelson, Charles Miers, Fernando Redígolo, Tereza Carvalho, Marcos Simplicio, Mats Näslund, and Makan Pourzandi. 2011. "A Quantitative Analysis of Current Security Concerns and Solutions for Cloud Computing." *Proceedings - 2011 3rd IEEE International Conference on Cloud Computing Technology and Science, CloudCom 2011* 231–38. doi: 10.1109/CloudCom.2011.39.
- Hashizume, Keiko, David G. Rosado, Eduardo Fernández-Medina, and Eduardo B. Fernandez. 2013. "An Analysis of Security Issues for Cloud Computing." *Journal of Internet Services and Applications* 4(1):5. doi: 10.1186/1869-0238-4-5.
- Holloway, Immy, and Les Todres. 2003. "The Status of Method: Flexibility, Consistency and Coherence." *Qualitative Research* 3(3):345–57. doi: 10.1177/1468794103033004.
- Indu, I., P. M. Rubesh Anand, and Vidhyacharan Bhaskar. 2018. "Identity and Access Management in Cloud Environment: Mechanisms and Challenges." *Engineering Science and Technology, an International Journal* 21(4):574–88. doi: 10.1016/j.jestch.2018.05.010.
- Larno, Sara, Ville Seppänen, and Jarkko Nurmi. 2019. "Method Framework for Developing Enterprise Architecture Security Principles." *Complex Systems Informatics and Modeling Quarterly* (20):57–71. doi: 10.7250/csimq.2019-20.03.
- Mahmood, Zaigham. 2011. "Cloud Computing for Enterprise Architectures: Concepts, Principles and Approaches." Pp. 3–19 in.
- Mahmood, Zaigham, and Richard Hill, eds. 2011. *Cloud Computing for Enterprise Architectures*. London: Springer London.
- McCambridge, Jim, John Witton, and Diana R. Elbourne. 2014. "Systematic Review of the Hawthorne Effect: New Concepts Are Needed to Study Research Participation Effects." *Journal of Clinical Epidemiology* 67(3):267–77. doi: 10.1016/j.jclinepi.2013.08.015.

- Mell, P. M., and T. Grance. 2011. *The NIST Definition of Cloud Computing*. Gaithersburg, MD.
- Modi, Chirag, Dhiren Patel, Bhavesh Borisaniya, Avi Patel, and Muttukrishnan Rajarajan. 2013. "A Survey on Security Issues and Solutions at Different Layers of Cloud Computing." *The Journal of Supercomputing* 63(2):561–92. doi: 10.1007/s11227-012-0831-5.
- Mogull, R., J. Arlen, F. Gilbert, A. Lane, D. Mortman, G. Peterson, and M. Rothman. 2009. *Security Guidance for Critical Areas of Focus in Cloud Computing*. Vol. 1.
- Motahari-Nezhad, Hamid R., Bryan Stephenson, and Sharad Singhal. 2009. "Outsourcing Business to Cloud Computing Services: Opportunities and Challenges." *IEEE Internet Computing* 10(4):1–17.
- Naresh Kumar, Sehgal, Bhatt Pramod Chandra p, and Acken John M. 2020. *Cloud Computing with Security - Concepts and Practices*.
- Nationaal Cyber Security Center. 2012. "Cloud Computing & Security."
- Newcombe, L. 2020. *Securing Cloud Services*.
- Nieves, Michael, Kelley Dempsey, and Victoria Yan Pillitteri. 2017. "NIST SP800-12 Revision 1 : An Introduction to Information Security." *NIST Special Publication* (800-12 (draft) revision 1).
- Niu, Dang-Dang, Lei Liu, Xin Zhang, Shuai Lü, and Zhuang Li. 2016. "Security Analysis Model, System Architecture and Relational Model of Enterprise Cloud Services." *International Journal of Automation and Computing* 13(6):574–84. doi: 10.1007/s11633-016-1014-2.
- Nowell, Lorelli S., Jill M. Norris, Deborah E. White, and Nancy J. Moules. 2017. "Thematic Analysis: Striving to Meet the Trustworthiness Criteria." *International Journal of Qualitative Methods* 16(1):160940691773384. doi: 10.1177/1609406917733847.
- Ose, Solveig Osborg. 2016. "Using Excel and Word to Structure Qualitative Data." *Journal of Applied Social Science* 10(2):147–62. doi: 10.1177/1936724416664948.
- Palo alto networks. 2020. *The State of Cloud Native Security*.
- Purohit, Kapila, and Anurag Rana. 2016. "Review: Authentication in Cloud Computing." *Internatinoal Journal Fo Scientific & Engineering Research* 7(7):744–46.
- Rahutomo, Faisal, Teruaki Kitasuka, and Masayoshi Aritsugi. 2012. "Semantic Cosine Similarity." P. 1 in *The 7th International Student Conference on Advanced Science and Technology ICAST*. Vol. 4.
- Rath, Annanda, Bojan Spasic, Nick Boucart, and Philippe Thiran. 2019. "Security Pattern for Cloud SaaS: From System and Data Security to Privacy Case Study in AWS and Azure." *Computers* 8(2):34. doi: 10.3390/computers8020034.
- Ryan, Gery W., and H. Russell Bernard. 2003. "Techniques to Identify Themes." *Field Methods* 15(1):85–109. doi: 10.1177/1525822X02239569.
- Safari, Fariba, Narges Safari, and Alireza Hasanzadeh. 2015. "The Adoption of Software-as-a-Service (SaaS): Ranking the Determinants." *Journal of Enterprise Information Management* 28(3):400–422. doi: 10.1108/JEIM-02-2014-0017.
- Saunders, M. N. K., P. Lewis, and A. Thornhill. 2019. *Research Methods for Business Students*. Pearson.
- Sherwood, John, Andrew Clark, and David Lynas. 2005. "Enterprise Security Architecture a Business-Driven Approach." *Computer Security Journal* 21(4).
- Spacy. 2021. "Spacy Industrial-Strengt Natural Language Processing." Retrieved (www.spacy.io).

- Subashini, S., and V. Kavitha. 2011. "A Survey on Security Issues in Service Delivery Models of Cloud Computing." *Journal of Network and Computer Applications* 34(1):1–11. doi: 10.1016/j.jnca.2010.07.006.
- Sun, Xiaotong. 2018. "Critical Security Issues in Cloud Computing: A Survey." Pp. 216–21 in *2018 IEEE 4th International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing, (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS)*. IEEE.
- Tan, P. N., M. Steinbach, and V. Kumar. 2005. *Introduction to Data Mining*. Boston: Addison Wesley.
- Tang, Changlong, and Jiqiang Liu. 2015. "Selecting a Trusted Cloud Service Provider for Your SaaS Program." *Computers & Security* 50:60–73. doi: <https://doi.org/10.1016/j.cose.2015.02.001>.
- The European Commission. 2020. "Towards a More Secure and Trusted Cloud in Europe." *The European Commission*. Retrieved (<https://ec.europa.eu/digital-single-market/en/news/towards-more-secure-and-trusted-cloud-europe>).
- The open group. 2016. *Open Group Guide Integrating Risk and Security within a TOGAF® Enterprise Architecture*.
- Van Velzen, D., M. De Jong, and S. Jansen. 2019. "Business Continuity Risks Through the Use of Software-As-A-Service: A Descriptive Survey."
- Weiyang, Kok, Duc Nghia Pham, Yasaman Eftekharypour, and Ang Jia Pheng. 2019. "Benchmarking NLP Toolkits for Enterprise Application." Pp. 289–94 in.
- van der Werff, Lisa, Grace Fox, Ieva Masevic, Vincent C. Emeakaroha, John P. Morrison, and Theo Lynn. 2019. "Building Consumer Trust in the Cloud: An Experimental Analysis of the Cloud Trust Label Approach." *Journal of Cloud Computing* 8(1):6. doi: 10.1186/s13677-019-0129-8.
- Westcott, T. 2005. *The Risks of Risk Management*.
- Yubico. 2021. *Cybersecurity in the Work from Anywhere Era*.



## Abbreviations

2FA	2 Factor Authentication
AVG	Algemene Verordening Gegevensbescherming (see GDPR)
CC	Cloud Computing
CCM	Cloud Controls Matrix
CSA	Cloud Security Alliance
CSC	Cloud Service Customer
CSP	CloudI Service Provider
EA	Enterprise Architecture
ESA	Enterprise Security Architecture
ENISA	European Network and Information Security Agency
GDPR	General Data Protection Regulation
IAAS	Infrastructure As A Service
ISO	International Organization for Standardization
NCSC	Nationaal Cyber Security Centrum
NEN	Dutch standard (NEderlandse Norm)
NIST	National Institute of Standards and Technology
NLP	Natural Language Processing
PAAS	Platform As A Service
SAAS	Software As A Service
SLA	Service Level Agreement
SME	Small and Medium sized Enterprise

## Appendix A: Overview of case organization

### Case organization 1:

Case organization 1 is a healthcare provider for plannable medical care in the Netherlands. Case organization 1 focusses on treatments in skin care, and is covered by the Dutch health insurance system. Additionally, case organization 1 offers specialist care in other area's, like Phlebology and Lymphology.

Case organization 1 office is located in the south of the Netherlands and employs around 40 people, of which 1 in the ICT department.

### Case organization 2:

Case organization 2 is a Dutch accountancy company that delivers a wide range of accounting and fiscal/legal services to ensure that the client's requirements in accounting, bookkeeping, administration, payroll and tax advisory are met.

Case organization 2 office is located in the south of the Netherlands and employs around 40 people, of which 1 in the ICT department.

### Case organization 3:

Case organization 3 is an ICT service provider for several public institutions that form a part of the city-region of the province of Limburg (NL), an agglomerate with about 25000 inhabitants and encompassing 8 municipalities.

Case organization 3 office is located in the south of the Netherlands and employs around 55 people.

## Appendix B: Overview of respondents

Name	Role	Relation with ESA/SAAS
Respondent 1	ICT manager/ICT administrator	Single Point of Contact for security and risk controls, Administrator for SAAS applications, assistant for audits
Respondent 2	ICT administrator	Administrator for SAAS applications, Network and infrastructure (security) administrator
Respondent 3	ICT administrator/technical application manager	Technical application manager for SAAS applications

## Appendix C: Survey/Interview information - protocol

### **SURVEY/INTERVIEW PROTOCOL**

Institute: Open Universiteit, faculteit Betawetenschappen  
Masteropleiding Business Process Management & IT

Degree programme: Open University of the Netherlands, Faculty of Science  
Master of Science Business Process Management & IT

Course: IM0602 BPMIT Graduation Assignment Preparation  
IM9806 Business Process Management and IT Graduation Assignment

Student: E. Mulkens

Identification number: 850993868

Date:

Thesis supervisor dr. Rik Bos

**Introduction: 10 minutes**

In preparation of the survey/interview, the respondent is given a brief explanation of the purpose of the survey/interview, the structure of the interview, the contribution expected from the respondents, the guidelines and privacy issues, the way that data is being collected and how data is being reported. (survey/interview and reports will be in Dutch language.)

**Purpose:**

General information about study course, student and purpose of survey/interview is given.

**Structure:**

During the survey closed questions are asked for the defined dimensions. The purpose for this is to have pre-defined answers to save time during the interview. During the semi-structured interview open questions are asked to corroborate the answers on the survey questions. The semi-structured interview also leaves room for further explanation and/or the possibility to ask questions about the subject.

**Contribution:**

Short explanation on how respondents will contribute to the research.

**Guidelines and privacy issues:**

- It is not mandatory to answer on questions, and there is always the option to stop the survey/interview
- The structure of the research is that per research element the practical situation of your own organization is looked at. This is done with closed survey questions and semi-structured interview questions.
- The results are processed anonymously and cannot be traced back.
- After agreement with the respondent the interview can be recorded, this to support validity and reliability of the research.

**Data collection:**

- Results are anonymized
- Analyzed and anonymized data will be made public, data cannot be traced back to persons or organization.

**Reporting:**

- All reports are anonymized
- Anonymized reports will be send to the respondent for review
- Final anonymized report will be send to the respondent

**Interview: 45 min**

During the interview the interview questions are discussed and checked for applicability in case-organization. Interview questions are in Dutch and are split up in following sections:

## Inhoud

Gebruikte afkortingen.....	
Algemeen.....	
Inleiding .....	
Definities.....	
Afstemming.....	
Ervaring SAAS en ESA.....	
Dimensies.....	
1. Compliance en regelgeving.....	
2. Identificatie, authenticatie en autorisatie .....	
3. Operationeel beheer en administratie .....	
4. Architectuur .....	
5. Toepassing van ESA.....	
Afsluiting.....	

### **Closing: 5 minutes**

At the end the respondent is being thanked for participation in this research and for providing additional information.

The final report with the results will be sent after completion of the investigation.

## Appendix D: Survey/Interview questions template

### **INTERVIEW VRAGEN/SCORE TEMPLATE**

Organisatie: XXX

Branche: xxxxxxxx

Respondent: RESPONDENT\_XXX

Datum: xx-xx-2021

Tijd: 99:99 – 99:99 uur

Opmerkingen:

Xxxxxxxx

xxxxxxxxxx

## **Inhoud**

Gebruikte afkortingen	42
Algemeen	43
Inleiding	43
Definities	43
Afstemming	43
Ervaring SAAS en ESA	43
Dimensies	43
1. Compliance en regelgeving	44
2. Identificatie, authenticatie en autorisatie	45
3. Operationeel beheer en administratie	46
4. Architectuur	47
5. Toepassing van ESA	48
Afsluiting	49



**Gebruikte afkortingen**

CC = Cloud Computing

ESA = Enterprise Security Architecture

SAAS = Software As A Service

CSP = Cloud Service Provider

CSC = Cloud Service Customer

## **Algemeen**

### Inleiding

Wat is uw positie binnen de organisatiestructuur?

Hoe groot is de organisatie?

Kunt u uw rol toelichten?

### Definities

Enterprise Security Architecture (ESA) is de praktijk van het toepassen van methoden voor het beschrijven van een (huidige en/of toekomstige) structuur van beveiligingsprocessen en informatiebeveiligingssystemen van een organisatie, zodat ze in overeenstemming zijn met de doelstellingen en de strategische richting van de organisatie.

Is deze definitie herkenbaar? Indien niet: wat is volgens u ESA?

Cloud computing (CC) is het via een netwerk – vaak het internet – op aanvraag beschikbaar stellen van hardware, software en gegevens, ongeveer zoals elektriciteit uit het lichtnet.

Is deze definitie herkenbaar? Indien niet: wat is volgens u Cloud Computing?

Software as a service (SAAS), ook weleens software on demand genoemd, is software die als een online dienst wordt aangeboden. De klant hoeft de software niet aan te schaffen, maar sluit bijvoorbeeld een contract per maand per gebruiker af.

Is deze definitie herkenbaar? Indien niet: wat is volgens u SAAS?

### Afstemming

Zijn doelstellingen voor ESA (risk en security controls) gekend en in documenten geformaliseerd?

Hoe helpt uw team bij het bereiken van de doelstellingen.

In hoeverre heeft u te maken gehad met incidenten betreffende risk en security?

### Ervaring SAAS en ESA

Met welke SAAS-applicaties heeft u al gewerkt?

Welke risk & security controls, gericht op SAAS, zijn er aanwezig binnen de organisatie?

Worden er standaarden/methodes/frameworks gebruikt voor inzet van ESA?

## **Dimensies**

## 1. Compliance en regelgeving

1.1. Voldoet de SAAS-oplossing(en) aan geldende wet- en regelgeving?

Schaal	Omschrijving
1	Volledig
2	Gedeeltelijk
3	Helemaal niet

Detail vragen:

1.1.1. Welk type gegevens worden er verwerkt binnen de SAAS-oplossing?

1.1.2. Welke specifieke regelgevingen gelden er voor uw branche/bedrijf ten aanzien van locatie, toegang, opslag en verwerking van data?

1.1.3. Wat is de impact voor de organisatie als regelgeving niet wordt nageleefd?

1.1.4. Vinden er periodiek audits plaats bij de CSP en bij de eigen organisatie?

1.1.5. Zijn de audits van de CSP beschikbaar voor inzage?

1.2. Worden gegevens in de SAAS applicatie(s) uitsluitend gebruikt of verwerkt in overeenstemming met het oorspronkelijke beoogde doel?

Schaal	Omschrijving
1	Ja
2	Nee

Detailvragen:

1.2.3. Wordt dit gegarandeerd door de CSP?

1.3. Is de toegang tot gegevens en de opslag van gegevens beveiligd middels encryptie?

Schaal	Omschrijving
1	Volledig
2	Gedeeltelijk
3	Helemaal niet

Detailvragen:

1.3.1. Wat zijn de gevolgen voor de organisatie als de encryptie niet veilig is?

1.3.2. Zijn er afspraken met de CSP en hoe zijn deze vastgelegd?

## 2. Identificatie, authenticatie en autorisatie

2.1. Moeten gebruikers van de SAAS-applicatie(s) zich authenticeren?

Schaal	Omschrijving
1	Ja
2	Nee

Detailvragen:

2.1.1. Welke authenticatie methode(s) worden gebruikt voor de aanmelding bij SAAS-applicaties?

2.1.2. Welk beleid geldt er bij eerste aanmelding (zelf aanmelden, op uitnodiging)?

2.1.3. Wat zijn de mogelijke gevolgen voor de organisatie als applicatie authenticatie niet veilig is?

2.2. Kan de SAAS-applicatie(s) de identiteit van de gebruiker vaststellen?

Schaal	Omschrijving
1	Volledig
2	Gedeeltelijk
3	Helemaal niet

Detailvragen:

2.2.1. Hoe wordt de identiteit van de gebruiker vastgesteld?

2.2.2. Wat zijn de gevolgen voor de organisatie als vaststelling niet juist is?

2.3. Is er een beleid voor toegang en gebruikscntrole?

Schaal	Omschrijving
1	Ja
2	Nee

Detailvragen:

- 2.3.1. Waar is dit beleid vastgelegd en hoe wordt dit gecontroleerd?
- 2.3.2. Wat zijn de gevolgen voor de organisatie als dit niet correct gebeurt?
- 2.3.3. Hoe is de organisatie van autorisatie ingericht (werken met super-users, gewone users, ...)?
- 2.3.4. Worden super-user accounts gecontroleerd?

### 3. Operationeel beheer en administratie

3.1 Wordt de beschikbaarheid van de SAAS-applicatie(s) gegarandeerd?

Schaal	Omschrijving
1	Volledig
2	Gedeeltelijk
3	Helemaal niet

Detailvragen:

- 3.1.1. Hoe wordt beschikbaarheid behouden in geval van cyber aanvallen?
- 3.1.2. Is er een uitwijkmogelijkheid naar een andere server-locatie in geval van calamiteiten?
- 3.1.3. Wat zijn de gevolgen voor de organisatie al er geen beschikbaarheid van de SAAS applicatie is?

3.2. Worden kwetsbaarheden in de SAAS-applicatie(s) gedetecteerd?

Schaal	Omschrijving
1	Ja
2	Nee

Detailvragen:

- 3.2.1. Zijn er automatische detectiesystemen voor kwetsbaarheden?
- 3.2.2. Hoe wordt de gebruiker/klant op de hoogte gebracht/gehouden?

3.3. Wordt er gebruik gemaakt van SLAs die ook security elementen bevatten?

Schaal	Omschrijving
1	Ja
2	Nee

Detailvragen:

3.3.1. Welke security elementen worden in de SLA beschreven?

3.3.2. Heeft u voorbeelden van SLAs die security elementen bevatten?

#### 4. Architectuur

4.1. Heeft u een beeld van de architectuur van de SAAS-applicatie(s)?

Schaal	Omschrijving
1	Volledig
2	Gedeeltelijk
3	Helemaal niet

Detailvragen:

4.1.1. Hoe zijn de componenten van de SAAS Cloud-applicatiearchitectuur met elkaar verbonden (via lokaal datacentrum of internet)?

4.1.2. Is de applicatie naast de gebruikelijke user interface ook via web-API-eindpunten te benaderen?

4.1.3. Wat is de impact indien ongeautoriseerde apparaten zich kunnen aanmelden bij de SAAS-applicatie(s)?

4.2. Bezit de CSP certificaten voor de SAAS applicaties?

Schaal	Omschrijving
1	Volledig
2	Gedeeltelijk
3	Helemaal niet

Detailvragen:

4.2.1. Welke certificaten zijn er?

4.2.2. Worden de certificaten ook periodiek vernieuwd?

4.3. Wordt de SAAS applicatie benaderd via beveiligingsprotocollen?

Schaal	Omschrijving
1	Volledig
2	Gedeeltelijk
3	Helemaal niet

4.3.1. Welke beveiligingsprotocollen worden er gebruikt?

4.3.2. Zijn deze beveiligingsprotocollen ook onderdeel van een SLA?

## 5. Toepassing van ESA

5.1 Gebruikt u ESA om de risico's van SAAS in kaart te brengen/te beheren?

Schaal	Omschrijving
1	Volledig
2	Gedeeltelijk
3	Helemaal niet

5.1.1. Zijn er functies/rollen in de organisatie die gerelateerd zijn aan ESA (CISO, security officer, Functionaris gegevensbeheer, ...) mbt SAAS?

5.1.2. Zijn er richtlijnen en principes voor implementatie van ESA bij SAAS?

5.1.3. Beschikt de case organisatie over een service portfolio (ISM/ITIL), waarin risk en security zaken mbt SAAS worden meegenomen?

5.2. Is er een budget voor risicobeheer en monitoring van SAAS applicaties?

Schaal	Omschrijving
1	Volledig
2	Gedeeltelijk
3	Helemaal niet

5.2.1. Zijn er medewerkers die uitsluitend belast zijn met beheer en monitoring van risk en security controls van (SAAS) applicaties?

Afsluiting

Uitleg vervolgtraject.

Hartelijk dank voor uw medewerking !



## Appendix E: Survey score

Nr	Onderdeel/dimensie	Normatieve uitspraak	Literatuur	Vraag	Score	Max Score	Gewicht	Score * Gewicht	Max Score * Gewicht	Score (%)
	Organisatie	CASE ORGANISATIE 1								
	Branche	Gezondheidszorg								
	Respondent	RESPONDENT1								
1.1	Compliance en regelgeving			Voldoet de SAAS-oplossing(en) aan geldende wet- en regelgeving?	50	100	1/3	16,67	33,33	50,0%
1.2	Compliance en regelgeving			Worden gegevens in de SAAS applicatie(s) uitsluitend gebruikt of verwerkt in overeenstemming met het oorspronkelijke beoogde doel?	100	100	1/3	33,33	33,33	100,0%
1.3	Compliance en regelgeving			Is de toegang tot gegevens en de opslag van gegevens beveiligd middels voorgeschreven encryptie methoden?	50	100	1/3	16,67	33,33	50,0%
1.	<b>Compliance en regelgeving sub totaal</b>	<b>De SAAS oplossing voldoet aan compliance en regelgeving</b>	<b>(Rath et al., 2019)</b>		<b>200</b>	<b>300</b>		<b>66,67</b>	<b>100,00</b>	<b>66,7%</b>
2.1	Identificatie, authenticatie en autorisatie			Moeten gebruikers van de SAAS-applicatie(s) zich authenticeren?	100	100	1/3	33,33	33,33	100,0%
2.2	Identificatie, authenticatie en autorisatie			Kan de SAAS-applicatie(s) de identiteit van de gebruiker vaststellen?	50	100	1/3	16,67	33,33	50,0%
2.3	Identificatie, authenticatie en autorisatie			Is er een beleid voor toegang en gebruikscntrole?	100	100	1/3	33,33	33,33	100,0%
2.	<b>Identificatie, authenticatie en autorisatie sub totaal</b>	<b>De SAAS oplossing voldoet aan identificatie, authenticatie en autorisatie vereisten</b>	<b>(Rath et al., 2019)</b>		<b>250</b>	<b>300</b>		<b>83,33</b>	<b>100,00</b>	<b>83,3%</b>
3.1	Operationeel beheer en administratie			Wordt de beschikbaarheid van de SAAS-applicatie(s) gegarandeerd?	50	100	1	50,00	100,00	50,0%
3.2	Operationeel beheer en administratie			Worden kwetsbaarheden in de SAAS-applicatie(s) gedetecteerd?	0	100	1/3	0,00	33,33	0,0%
3.3	Operationeel beheer en administratie			Wordt er gebruik gemaakt van SLA's die ook security elementen bevatten?	0	100	1/3	0,00	33,33	0,0%
3.	<b>Operationeel beheer en administratie sub totaal</b>	<b>Operationeel beheer en administratie voldoet aan vereisten</b>	<b>(Hashizume et al., 2013) (Rath et al., 2019)</b>		<b>50</b>	<b>100</b>		<b>50,00</b>	<b>100,00</b>	<b>50,0%</b>
4.1	Architectuur			Heeft u een beeld van de architectuur van de SAAS-applicatie(s)?	50	100	1/3	16,67	33,33	50,0%
4.2	Architectuur			Bezit de CSP certificaten voor de SAAS applicaties?	50	100	1/3	16,67	33,33	50,0%
4.3	Architectuur			Wordt de SAAS applicatie benaderd via beveiligingsprotocollen?	100	100	1/3	33,33	33,33	100,0%
4.	<b>Architectuur sub totaal</b>	<b>Architectuur is inzichtelijk</b>	<b>(Mahmood, 2011) (Rath et al., 2019)</b>		<b>200</b>	<b>300</b>		<b>66,67</b>	<b>100,00</b>	<b>66,7%</b>
5.1	Toepassing van ESA			Gebruikt u ESA om de risico en security van SAAS in kaart te brengen/te beheren?	50	100	1/2	25,00	50,00	50,0%
5.2	Toepassing van ESA			Is er een budget voor risicobeheer en monitoring van SAAS applicaties?	50	100	1/2	25,00	50,00	50,0%
5.	<b>Toepassing van ESA</b>	<b>Risico en security wordt middels ESA in kaart gebracht en beheerd</b>	<b>(Larno et al., 2019)</b>		<b>100</b>	<b>200</b>		<b>50,00</b>	<b>100,00</b>	<b>50,0%</b>

Organisatie	CASE ORGANISATIE 2		
Branche	Accountancy		
Respondent	RESPONDENT2		

Nr	Onderdeel/dimensie	Normatieve uitspraak	Literatuur	Vraag	Score	Max Score	Gewicht	Score * Gewicht	Max Score * Gewicht	Score (%)
1.1	Compliance en			Voldoet de SAAS-oplossing(en) aan geldende wet- en	50	100	1/3	16,67	33,33	50,0%
1.2	Compliance en regelgeving			Worden gegevens in de SAAS applicatie(s) uitsluitend gebruikt of verwerkt in overeenstemming met het oorspronkelijke beoogde	100	100	1/3	33,33	33,33	100,0%
1.3	Compliance en regelgeving			Is de toegang tot gegevens en de opslag van gegevens beveiligd middels voorgeschreven encryptie methoden?	100	100	1/3	33,33	33,33	100,0%
1.	<b>Compliance en regelgeving subtotaal</b>	<b>De SAAS oplossing voldoet aan compliance en regelgeving</b>	<b>(Rath et al., 2019)</b>		<b>250</b>	<b>300</b>		<b>83,33</b>	<b>100,00</b>	<b>83,3%</b>
2.1	Identificatie, authenticatie en			Moeten gebruikers van de SAAS-applicatie(s) zich authenticeren?	100	100	1/3	33,33	33,33	100,0%
2.2	Identificatie, authenticatie en			Kan de SAAS-applicatie(s) de identiteit van de gebruiker vaststellen?	50	100	1/3	16,67	33,33	50,0%
2.3	Identificatie, authenticatie en			Is er een beleid voor toegang en gebruikscntrole?	100	100	1/3	33,33	33,33	100,0%
2.	<b>Identificatie, authenticatie en autorisatie subtotaal</b>	<b>De SAAS oplossing voldoet aan identificatie, authenticatie en autorisatie vereisten</b>	<b>(Rath et al., 2019)</b>		<b>250</b>	<b>300</b>		<b>83,33</b>	<b>100,00</b>	<b>83,3%</b>
3.1	Operationeel beheer en administratie			Wordt de beschikbaarheid van de SAAS-applicatie(s) gegarandeerd?	50	100	1	50,00	100,00	50,0%
3.2	Operationeel beheer en administratie			Worden kwetsbaarheden in de SAAS-applicatie(s) gedetecteerd?	0	100	1/3	0,00	33,33	0,0%
3.3	Operationeel beheer en administratie			Wordt er gebruik gemaakt van SLA's die ook security elementen bevatten?	0	100	1/3	0,00	33,33	0,0%
3.	<b>Operationeel beheer en administratie subtotaal</b>	<b>Operationeel beheer en administratie voldoet aan vereisten</b>	<b>(Hashizume et al., 2013) (Rath et al., 2019)</b>		<b>50</b>	<b>100</b>		<b>50,00</b>	<b>100,00</b>	<b>50,0%</b>
4.1	Architectuur			Heeft u een beeld van de architectuur van de SAAS-applicatie(s)?	0	100	1/3	0,00	33,33	0,0%
4.2	Architectuur			Bezit de CSP certificaten voor de SAAS applicaties?	50	100	1/3	16,67	33,33	50,0%
4.3	Architectuur			Wordt de SAAS applicatie benaderd via beveiligingsprotocollen?	100	100	1/3	33,33	33,33	100,0%
4.	<b>Architectuur subtotaal</b>	<b>Architectuur is inzichtelijk</b>	<b>(Mahmood, 2011) (Rath et al., 2019)</b>		<b>150</b>	<b>300</b>		<b>50,00</b>	<b>100,00</b>	<b>50,0%</b>
5.1	Toepassing van ESA			Gebruikt u ESA om de risico's van SAAS in kaart te brengen/te	0	100	1/2	0,00	50,00	0,0%
5.2	Toepassing van ESA			Is er een budget voor risicobeheer en monitoring van SAAS	50	100	1/2	25,00	50,00	50,0%
5.	<b>Toepassing van ESA</b>	<b>Risico en security wordt middels ESA in kaart gebracht en beheerd</b>	<b>(Larno et al., 2019)</b>		<b>50</b>	<b>200</b>		<b>25,00</b>	<b>100,00</b>	<b>25,0%</b>

Organisatie	CASE ORGANISATIE 3		
Branche	Overheid		
Respondent	RESPONDENT3		

Nr	Onderdeel/dimensie	Normatieve uitspraak	Literatuur	Vraag	Score	Max Score	Gewicht	Score * Gewicht	Max Score * Gewicht	Score (%)
1.1	Compliance en regelgeving			Voldoet de SAAS-oplossing(en) aan geldende wet- en regelgeving?	100	100	1/3	33,33	33,33	100,0%
1.2	Compliance en regelgeving			Worden gegevens in de SAAS applicatie(s) uitsluitend gebruikt of verwerkt in overeenstemming met het oorspronkelijke beoogde doel?	100	100	1/3	33,33	33,33	100,0%
1.3	Compliance en regelgeving			Is de toegang tot gegevens en de opslag van gegevens beveiligd middels voorgeschreven encryptie methoden?	50	100	1/3	16,67	33,33	50,0%
1.	<b>Compliance en regelgeving sub totaal</b>	<b>De SAAS oplossing voldoet aan compliance en regelgeving</b>	<b>(Rath et al., 2019)</b>		<b>250</b>	<b>300</b>		<b>83,33</b>	<b>100,00</b>	<b>83,3%</b>
2.1	Identificatie, authenticatie en autorisatie			Moeten gebruikers van de SAAS-applicatie(s) zich authenticeren?	100	100	1/3	33,33	33,33	100,0%
2.2	Identificatie, authenticatie en autorisatie			Kan de SAAS-applicatie(s) de identiteit van de gebruiker vaststellen?	50	100	1/3	16,67	33,33	50,0%
2.3	Identificatie, authenticatie en autorisatie			Is er een beleid voor toegang en gebruikscntrole?	100	100	1/3	33,33	33,33	100,0%
2.	<b>Identificatie, authenticatie en autorisatie sub totaal</b>	<b>De SAAS oplossing voldoet aan identificatie, authenticatie en autorisatie vereisten</b>	<b>(Rath et al., 2019)</b>		<b>250</b>	<b>300</b>		<b>83,33</b>	<b>100,00</b>	<b>83,3%</b>
3.1	Operationeel beheer en administratie			Wordt de beschikbaarheid van de SAAS-applicatie(s) gegarandeerd?	100	100	1/3	33,33	33,33	100,0%
3.2	Operationeel beheer en administratie			Worden kwetsbaarheden in de SAAS-applicatie(s) gedetecteerd?	100	100	1/3	33,33	33,33	100,0%
3.3	Operationeel beheer en administratie			Wordt er gebruik gemaakt van SLA's die ook security elementen bevatten?	100	100	1/3	33,33	33,33	100,0%
3.	<b>Operationeel beheer en administratie sub totaal</b>	<b>Operationeel beheer en administratie voldoet aan vereisten</b>	<b>(Hashizume et al., 2013) (Rath et al., 2019)</b>		<b>300</b>	<b>300</b>		<b>100,00</b>	<b>100,00</b>	<b>100,0%</b>
4.1	Architectuur			Heeft u een beeld van de architectuur van de SAAS-applicatie(s)?	50	100	1/3	16,67	33,33	50,0%
4.2	Architectuur			Bezit de CSP certificaten voor de SAAS applicaties?	100	100	1/3	33,33	33,33	100,0%
4.3	Architectuur			Wordt de SAAS applicatie benaderd via beveiligingsprotocollen?	100	100	1/3	33,33	33,33	100,0%
4.	<b>Architectuur sub totaal</b>	<b>Architectuur is inzichtelijk</b>	<b>(Mahmood, 2011) (Rath et al., 2019)</b>		<b>250</b>	<b>300</b>		<b>83,33</b>	<b>100,00</b>	<b>83,3%</b>
5.1	Toepassing van ESA			Gebruikt u ESA om de risico en security van SAAS in kaart te brengen/te beheren?	50	100	1/2	25,00	50,00	50,0%
5.2	Toepassing van ESA			Is er een budget voor risicobeheer en monitoring van SAAS	50	100	1/2	25,00	50,00	50,0%
5.	<b>Toepassing van ESA</b>	<b>Risico en security wordt middels ESA in kaart gebracht en beheerd</b>	<b>(Larno et al., 2019)</b>		<b>100</b>	<b>200</b>		<b>50,00</b>	<b>100,00</b>	<b>50,0%</b>

## Appendix F: Determination of similarities/differences and common themes

Nr	Nr intern	Vraag	Interview 1	Interview 2	Interview 3	Spacy12	Spacy13	Spacy23	Similarities/Difference	Theme	Theme	Theme	Theme
1	I1	Wat is uw positie binnen de organisatiestructuur?	Externe ik beheerder/adviseur	Externe ik beheerder/adviseur	Medewerker ICT/technisch applicatiebeheerder	1,00	0,25	0,25	externe IT beheerder	T1 Small and Medium sized Enterprise			
2	I2	Hoe groot is de organisatie?	40 medewerkers	40 medewerkers	55 medewerkers	1,00	0,83	0,83	vergelijk-bare organisatieomvang	T1 Small and Medium sized Enterprise			
3	I3	Kunt u uw rol toelichten?	Systeembeheer en applicatie beheer	Systeembeheer en applicatie beheer	Applicatiebeheer (installatie en onderhoud) up to date houden van systemen, verhelpen storingen	1,00	0,53	0,53	systeembeheer en applicatiebeheer				
4	D1	Enterprise Security Architecture (ESA) is de praktijk van het toepassen van methoden voor het beschrijven van een (fluidige en/of toekomstige) structuur van beveiligingsprocessen en informatiebeveiligingsystemen van een organisatie, zodat ze in overeenstemming zijn met de doelstellingen en de strategische richting van de organisatie. Is deze definitie herkenbaar? Indien niet, wat is volgens u ESA?	Ja, over welke doelstellingen hebben we het hier	herkenbaar, over welke doelstellingen hebben we het hier?	Prima definitie, herkenbaar	0,41	0,40	0,19	ESA definitie herkenbaar	T2 Clear understanding of definition			
5	D2	Cloud computing (CC) is het via een netwerk - vaak het internet - op aanvraag beschikbaar stellen van hardware, software en gegevens, ongeveer zoals elektriciteit uit het lichtnet. Is deze definitie herkenbaar? Indien niet, wat is volgens u Cloud Computing?	Herkenbaar	Ja, duidelijk en herkenbaar	Herkenbaar, ok	0,79	0,51	0,70	cloud computing definitie herkenbaar	T2 Clear understanding of definition			
6	D3	Software as a service (SAAS), ook wel eens software on demand genoemd, is software die als een online dienst wordt aangeboden. De klant hoeft de software niet aan te schaffen, maar sluit bijvoorbeeld een contract per maand per gebruiker af. Is deze definitie herkenbaar? Indien niet, wat is volgens u SAAS?	JA, prima definitie	JA, prima definitie	Duidelijk	1,00	0,60	0,60	SAAS definitie duidelijk	T2 Clear understanding of definition			

7	A1	Zijn doelstellingen voor ESA (risk en security controls) gekend en in documenten geformaliseerd?	NEN7510 / ISO / AVG vastgelegd in AAVV online tool en intern DMS		Controls zijn vastgelegd op management niveau, ITIL, SLA's,	0,20	-0,01	0,28	ESA doelstellingen zijn vastgelegd/geformaliseerd, maar voor iedere case organisatie op een andere manier	T3 ESA goals	T8 ESA is used to a very limited extent	T26 limited budget for risk management and monitoring of applications	
8	A2	Hoe helpt uw team bij het bereiken van de doelstellingen.	Controle beveiligingsinstellingen lokale en SAAS applicaties, netwerkapparatuur (firewall, switch), computers en servers.	beveiligingsinstelling en lokale en SAAS applicaties, netwerkapparatuur (firewall, switch), computers en (RDP) servers	Confirmatie aan beschreven zaken die door management zijn vastgelegd middels papers	0,90	0,58	0,44	controle beveiligingsinstellingen confirmatie aan management documenten	T4 policy and guidelines for access and usage of SAAS applications	T8 ESA is used to a very limited extent		
9	A3	In hoeverre heeft u te maken gehad met incidenten betreffende risk en security?	Ransomware aanval die veel impact heeft gehad op de organisatie en medewerkers, gebruikers noteren wel eens wachtwoorden op papier en deze worden dan bij de computer bewaard, medewerkers die elkaar proberen te helpen door gebruikersgegevens te delen.	Virus aanval	Tijdig aanpassen van wachtwoorden (direct na installatie)...is vastgelegd in procedure maar wordt niet altijd gevolgd... Hacks, poging tot gebeurt regelmatig...maar worden tijdig gedetecteerd...	0,45	0,64	0,34	aanvallen (ransomware, virus, hacks)	T5 sensitive data leak			
10	E1	Met welke SAAS-applicaties heeft u al gewerkt?	Office 365 Mail, Zorgmail, AAVV AVG tool (deze bevat de onderdelen en registratie van AVG en NEN7510 richtlijnen), Vecozo (verzekeringscheck voor patiënten), Snelstart (financiële administratie, boekhouding), eDevOp (financiële administratie specifiek voor huidtherapie).	Google Gsuite (Mail), Elsevier Nextens, UNIT4, Fiscaal Gemak, HR Salaris Gemak, Boekhoud Gemak, Multiverse Online, diverse RDP servers van klanten, Belastingdienst, Duo Security	Microsoft office 365, provider van overheidsapplicaties die via internet wordt aangeboden (aangiftes, verhuizingen, bouw aanvragen, etc...) Deze applicaties gaan steeds meer over naar SAAS..	0,72	0,78	0,87	meerder SAAS applicaties in gebruik, ook voor core business activiteiten	T6 Core business SAAS application	T15 Availability of SAAS applications was a crucial aspect		
11	E2	Welke risk & security controls, gericht op SAAS, zijn er aanwezig binnen de organisatie?	Gebruikers attenderen op phishing (met name Office 365). Controle toegangsrechten (autorisatie).	gebruikers attenderen op phishing (met name Google Gsuite) controle toegangsrechten (autorisatie)	Gebruik dmz zones, Reverse proxy, gebruik van certificaten, afdwingen sterke wachtwoorden,	0,92	0,50	0,43	controle autorisatie phishing waarschuwing, wachtwoordbeleid	T7 Risk & security controls			

12	E3	Worden er standaarden/methodes/frameworks gebruikt voor inzet van ESA?	NEN7510 (dit zijn officiële richtlijnen waaraan de organisatie moet voldoen en waarop de organisatie ook ge-audit wordt.	Moet ik navragen	Niet bekend, audit so, avg, specifieke regels voor overheden, Specifiek system voor overheden ten behoeve van functiescheiding, wachtwoorden, etc	0,43	0,70	0,45	Geen breed gebruik van frameworks voor ESA	T8 ESA is used to a very limited extent			
13	1.1	Voldoet de SAAS-oplossing(en) aan geldende wet- en	Gedeeltelijk	Gedeeltelijk	Volledig	1,00	0,68	0,68	SAAS voldoet aan wet-en regelgeving	T9 strict regulations for access and data storage			
14	1.1.1	Welk type gegevens worden er verwerkt binnen de SAAS-oplossing?	Persoonsgegevens, medische gegevens, financiële gegevens	Persoonsgegevens, financiële gegevens	Persoonsgegevens, kadastrale gegevens, financiële gegevens, MS office data.	0,93	0,90	0,88	SAAS voldoet aan wet-en regelgeving (persoon, medisch, financieel)	T5 sensitive data leak			
15	1.1.2	Welke specifieke regelgevingen gelden er voor uw branche/bedrijft en aanzien van locatie, toegang, opslag en verwerking van data?	NEN 7510 voor informatiebeveiliging. De maatregelen zijn best practices die afhankelijk van het risicoprofiel van de zorginstelling en haar beleidsuitgangspunten gebruikt kunnen worden. Slechts de audit is verplicht en deze wordt uitgevoerd op basis van de door de zorginstelling zelf opgezette norm. Hierbij geldt het principe 'Pas toe of leg uit'. Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz): Elke zorgverlener is vanaf juli 2017 verplicht om zijn cliënten te informeren over de elektronische	Handleiding Regelgeving Accountancy (HRA): <a href="https://www.nba.nl/tools/hra-2021/">https://www.nba.nl/tools/hra-2021/</a> HRA editie 2021 met de relevante wet- en regelgeving voor accountants. Deze uitgave bevat wetgeving, een EU-verordening en EU-richtlijn, verordeningen en nadere voorschriften waaronder de Nadere voorschriften controle- en overige standaarden. Zo heeft een accountant alle regelgeving bij elkaar.	Dit is vastgelegd in verwerkersovereenkomst, SLA's	0,88	0,31	0,34	Elke branche heeft andere specifieke regelgeving (medisch, financieel, overheid)	T9 strict regulations for access and data storage			

12	E3	Worden er standaarden/methodes/frameworks gebruikt voor inzet van ESA?	NEN7510 (dit zijn officiële richtlijnen waaraan de organisatie moet voldoen en waarop de organisatie ook ge-audit wordt.	Moet ik navragen	Niet bekend, audit so, avg, specifieke regels voor overheden, Specifiek system voor overheden ten behoeve van functiescheiding, wachtwoorden, etc	0,43	0,70	0,45	Geen breed gebruik van frameworks voor ESA	T8 ESA is used to a very limited extent			
13	1.1	Voldoet de SAAS-oplossing(en) aan geldende wet- en	Gedeeltelijk	Gedeeltelijk	Volledig	1,00	0,68	0,68	SAAS voldoet aan wet-en regelgeving	T9 strict regulations for access and data storage			
14	1.1.1	Welk type gegevens worden er verwerkt binnen de SAAS-oplossing?	Persoonsgegevens, medische gegevens, financiële gegevens	Persoonsgegevens, financiële gegevens	Persoonsgegevens, kadastrale gegevens, financiële gegevens, MS office data.	0,93	0,90	0,88	SAAS voldoet aan wet-en regelgeving (persoon, medisch, financieel)	T5 sensitive data leak			
15	1.1.2	Welke specifieke regelgevingen gelden er voor uw branche/bedrijft en aanzien van locatie, toegang, opslag en verwerking van data?	NEN 7510 voor informatiebeveiliging. De maatregelen zijn best practices die afhankelijk van het risicoprofiel van de zorginstelling en haar beleidsuitgangspunten gebruikt kunnen worden. Slechts de audit is verplicht en deze wordt uitgevoerd op basis van de door de zorginstelling zelf opgezette norm. Hierbij geldt het principe 'Pas toe of leg uit'. Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz): Elke zorgverlener is vanaf juli 2017 verplicht om zijn cliënten te informeren over de elektronische	Handleiding Regelgeving Accountancy (HRA): <a href="https://www.nba.nl/tools/hra-2021/">https://www.nba.nl/tools/hra-2021/</a> HRA editie 2021 met de relevante wet- en regelgeving voor accountants. Deze uitgave bevat wetgeving, een EU-verordening en EU-richtlijn, verordeningen en nadere voorschriften waaronder de Nadere voorschriften controle- en overige standaarden. Zo heeft een accountant alle regelgeving bij elkaar.	Dit is vastgelegd in verwerkersovereenkomst, SLA's	0,88	0,31	0,34	Elke branche heeft andere specifieke regelgeving (medisch, financieel, overheid)	T9 strict regulations for access and data storage			

16	1.1.3.	Wat is de impact voor de organisatie als regelgeving niet wordt nageleefd?	Wat is de impact voor de organisatie als regelgeving niet wordt nageleefd? AVG boetes, boetes Inspectie voor de Gezondheidszorg, (indirect: negatief in media en bij andere verwijzende	AVG boetes, boetes Autoriteit Financiële Markten (AFM), boetes Belastingdienst	Datalek met alle gevolgen van dien (media)	0,85	0,70	0,73	boetes, mediabericht (imageschade)	T5 sensitive data leak		
17	1.1.4.	Vinden er periodiek audits plaats bij de CSP en bij de eigen organisatie?	Audits bij Microsoft, Zorgmail, Vecozo, Snelstart waarschijnlijk wel. Case organisatie krijgt jaarlijkse ZKN audit.	Audits bij Google: <a href="https://cloud.google.com/security/compliance/">https://cloud.google.com/security/compliance/</a> An independent third party auditor has granted a formal certification, attestation, or audit report based on an assessment that affirms our compliance with these offerings. Unit4 krijgt waarschijnlijk ook audits. Duo Security krijgt een Service Organization Control 2 (SOC 2) audit van Security en Confidentiality. Case organisatie krijgt jaarlijkse ??? audit	Ja, jaarlijkse audit (organisatie?) BMC?	0,52	0,44	0,56	audits bij Provider en klant	T10 subject to periodic audits	T11 relied on the compliance information from the certified SAAS CSP	
18	1.1.5.	Zijn de audits van de CSP beschikbaar voor inzage?	Geen idee.	Geen idee	MS Office 365 ? Audits die intern worden uitgevoerd zijn beschikbaar voor inzage voor de afnemer	0,63	0,21	0,15	Inzage audits niet duidelijk	T10 subject to periodic audits	T11 relied on the compliance information from the certified SAAS CSP	
19	1.2.	Worden gegevens in de SAAS applicatie(s) uitsluitend gebruikt of verwerkt in overeenstemming met het oorspronkelijke beoogde	Ja	Ja	Ja	1,00	1,00	1,00	saas gegevens worden uitsluitend gebruikt voor beoogde doel	T12 Privacy		



20	1.2.1	Wordt dit gegarandeerd door de CSP?	-Waarschijnlijk wel door de Nederlandse leveranciers. Microsoft zou moeten voldoen aan Europese AVG richtlijnen.	Waarschijnlijk wel door de Nederlandse leveranciers die specifieke SAAS applicaties leveren voor financiële dienstverleners. Google zou moeten voldoen aan Europese AVG richtlijnen.	Ja, dit wordt gegarandeerd	0,94	0,52	0,58	Garantie doel datagebruik gegarandeerd door AVG voorschriften	T11 relied on the compliance information from the certified SAAS CSP			
21	1.3	Is de toegang tot gegevens en de opslag van gegevens beveiligd middels encryptie?	Gedeeltelijk	Volledig	Gedeeltelijk	0,68	1,00	0,68	toegang en opslag gegevens gedeeltelijk beveiligd met encryptie lekken data	T13 electronic authentication of humans in a SAAS application was a problem			
22	1.3.1	Wat zijn de gevolgen voor de organisatie als de encryptie niet veilig is?	Gegevens van patienten kunnen worden gelekt (datalek). Boetes mogelijk, zelfs stilleggen van activiteiten door Zorgautoriteiten is mogelijk, tevens negatieve berichtgeving in media	Gegevens van klanten worden gelekt. Boetes mogelijk, zelfs stilleggen van activiteiten door ??? is mogelijk	Ingeval van een hack zou dit een probleem opleveren vanwege het feit dat ze niet encrypted zijn.	0,53	0,73	0,62		T13 electronic authentication of humans in a SAAS application was a problem	T5 sensitive data leak		
23	1.3.2	Zijn er afspraken met de CSP en hoe zijn deze vastgelegd?	niet bekend	niet bekend	Weet ik niet	0,67	0,07	0,24	vastlegging van afspraken met CSP niet duidelijk	T11 relied on the compliance information from the certified SAAS CSP			
24	2.1	2.1 Moeten gebruikers van de SAAS-applicatie(s) zich authenticeren?	Ja	Ja	Ja	1,00	1,00	1,00	gebruikers moeten zich authenticeren	T14 Available registration policy			
25	2.1.1	Welke authenticatie methode(s) worden gebruikt voor de aanmelding bij SAAS-applicaties?	Wachtwoord/gebruikersnaam, 2FA	wachtwoord/gebruikersnaam, 2FA (Duo Security)	Buiten kantoor 2FA middels smartphone, verder gebruikersnaam/wachtwoord...voornamelijk geregeld via SSD.	0,33	0,62	0,19	2FA wordt beperkt gebruikt	T13 electronic authentication of humans in a SAAS application was a problem			
26	2.1.2	Welk beleid geldt er bij eerste aanmelding (zelf aanmelden, op uitnodiging)?	Op uitnodiging, na aanmaak van account door beheerder. In sommige SAAS applicaties wordt gewerkt met	Op uitnodiging, na aanmaak van account door beheerder	Beleid is voornamelijk via SSD en via startmenu/snelkoppeling in geval van nieuwe applicatie	0,73	0,64	0,66	eerste aanmelding op uitnodiging of via SSD	T14 Available registration policy			

27	2.1.3.	Wat zijn de mogelijke gevolgen voor de organisatie als applicatie authenticatie niet veilig is?	Accounts kunnen worden gehackt, AVG/Zorgautoriteit boetes, Datalek met verstrekking van gegevens, negatieve berichtgeving in de media en bij patiënten.	Accounts kunnen worden gehackt, AVG boetes De Autoriteit Persoonsgegevens tekende sinds 2016 meeste datalekken op voor de accountancy- en finance sector. Samen met de zorgsector staan ze op dat gebied eenzaam bovenaan. Financiële informatie is natuurlijk erg privacygevoelig, maar ook het BSN is erg gewild. Bijvoorbeeld voor identiteitsfraude	Datalek met alle gevolgen van dien	0,88	0,66	0,55	hack of datalek wanneer authenticatie niet veilig is	T13 electronic authentication of humans in a SAAS application was a problem	T5 sensitive data leak		
28	2.2.	Kan de SAAS-applicatie(s) de identiteit van de gebruiker vaststellen?	Gedeeltelijk	Gedeeltelijk	Gedeeltelijk	1,00	1,00	1,00	identiteit gebruiker kan gedeeltelijk worden vastgesteld	T13 electronic authentication of humans in a SAAS application was a problem			
29	2.2.1.	Hoe wordt de identiteit van de gebruiker vastgesteld?	Ingeval van 2FA via smartphone. Persoonlijke overhandiging van inloggegevens aan medewerker.	Ingeval van 2FA via smartphone. Persoonlijke overhandiging van inloggegevens aan medewerker.	Extern via 2FA (smartphone), intern via SSD user-id/pw., aparte inlog voor bepaalde applicaties	1,00	0,64	0,64	identiteit vaststelling beperkt via 2FA	T13 electronic authentication of humans in a SAAS application was a problem			
30	2.2.2.	Wat zijn de gevolgen voor de organisatie als vaststelling niet juist is?	Accounts kunnen worden gehackt, AVG/Zorgautoriteit boetes, Datalek met verstrekking van gegevens, negatieve	Accounts kunnen worden gehackt, AVG boetes	Datalek met alle gevolgen van dien	0,81	0,66	0,53	hacks of datalek wanneer identiteit controle mislukt	T13 electronic authentication of humans in a SAAS application was a problem	T5 sensitive data leak		
31	2.3.	Is er een beleid voor toegang en gebruikscapaciteit?	Ja	Ja	Ja	1,00	1,00	1,00	gebruik voor toegangsbeheer is aanwezig	T4 policy and guidelines for access and usage of SAAS applications			
32	2.3.1.	Waar is dit beleid vastgelegd en hoe wordt dit gecontroleerd?	Vastgelegd in toegangsbeheer document binnen intern DMS systeem	Vastgelegd in toegangsbeheer document	Active directory beleid (security groepen, etc.), autorisatie formulieren voor het toekennen van rechten op basis van functieprofielen	0,93	0,73	0,68	toegangsbeheer vastgelegd in document	T4 policy and guidelines for access and usage of SAAS applications			

33	2.3.2	Wat zijn de gevolgen voor de organisatie als dit niet correct gebeurt?	Ongeautoriseerde toegang tot patiëntgegevens	Ongeautoriseerde toegang tot klantgegevens	Kan leiden tot datalek	0,95	0,54	0,57	datalek, niet geautoriseerde toegang	T5 sensitive data leak		
34	2.3.3	Hoe is de organisatie van autorisatie ingericht (werken met super-users, gevone users, ...)?	Systeembeheerder geeft medewerkers toegang tot applicaties op verzoek van kliniek manager. Toegangsbeheer document bevat: vereiste accounts, rollen en Access Control List (hiering worden bijvoorbeeld ook de certificaten van medewerkers	Systeembeheerder geeft medewerkers toegang tot applicaties op verzoek van manager. Toegangsbeheer document bevat: vereiste accounts, rollen en ACL binnen elke (SAAS-)applicatie	Super-users (aanvragen en uitdelen van autorisaties), key-users (aanvragen en bredere atherosatie) en gevone users (specifiek per functie/werkzaamheden)... er is functiescheiding	0,96	0,69	0,56	autorisatie organisatie onderveeld in user groepen (super users, gevone users)	T4 policy and guidelines for access and usage of SAAS applications		
35	2.3.4	Worden super-user accounts gecontroleerd?	Niet	Niet	Niet	1,00	1,00	1,00	Geen controle super user accounts	T13 electronic authentication of humans in a SAAS application was a problem		
36	3.1	Wordt de beschikbaarheid van de SAAS-applicatie(s) gegarandeerd?	Gedeeltelijk, tot beperkte up-time	Gedeeltelijk	Volledig	0,76	0,61	0,68	beschikbaarheid SAAS gedeeltelijk gegarandeerd	T15 Availability of SAAS applications was a crucial aspect	T27 limited operational up time	T30 limited confidence that SAAS solutions meet the requirements
37	3.1.1	Hoe wordt beschikbaarheid behouden in geval van cyber aanvallen?	Bedoel je aanvallen op SAAS leverancier of ook aanvallen op klant?? Office 365: load-balancing/failover naar andere server-locaties. Andere SAAS niet bekend.	Google GSuite: load-balancing/failover naar andere server-locaties.	Fail over server, back-ups, procedures zijn vastgelegd in documenten, calamiteitenplan	0,95	0,45	0,43	beschikbaarheid garantie via fail over	T15 Availability of SAAS applications was a crucial aspect		
38	3.1.2	Is er een uitwijkmogelijkheid naar een andere server-locatie in geval van calamiteiten?	Office365 wel, andere Saas niet bekend	Google GSuite wel, andere Saas niet bekend	Alles is dubbel uitgevoerd op twee fysieke locaties (gesplitst)	0,69	0,47	0,30	uitwijkmogelijkheid naar andere server-locatie	T16 Availability of fail-over		
39	3.1.3	Wat zijn de gevolgen voor de organisatie als er geen beschikbaarheid van de SAAS applicatie is?	Financiële administratie kan niet worden bijgehouden. Geen mailverkeer mogelijk. Geen elektronische berichtuitwisseling met	Moet ik navragen	Applicaties zijn dan niet bereikbaar en dat heeft gevolgen voor afwerken van workload	0,31	0,51	0,48	dageijkse werkzaamheden worden beperkt of onmogelijk	T15 Availability of SAAS applications was a crucial aspect		
40	3.2	Worden kwetsbaarheden in de SAAS-applicatie(s) gedetecteerd?			Ja	1,00	0,00	0,00	Kwetsbaarheden worden beperkt gedetecteerd	T17 not clear if there was any ability of detection of vulnerabilities that could impact SAAS applications	T5 sensitive data leak	T31 No up to date insights in the amount and severity of security vulnerabilities and threats

41	3.2.1	Zijn er automatische detectiesystemen voor kwetsbaarheden?	Office 365 waarschijnlijk wel, andere weet ik niet.	Google Gsuite wel, andere niet bekend	Ja, er zijn procedures die dit regelen	0.73	0.53	0.60	Er zijn automatische detectiesystemen, maar niet duidelijk bekend bij klant	T17 not clear if there was any ability of detection of vulnerabilities that could impact SAAS applications	T31 No up to date insights in the amount and severity of security vulnerabilities and threats	
42	3.2.2	Hoe wordt de gebruiker/klant op de hoogte gebracht/gehouden?	Waarschijnlijk achteraf na detectie van aanval (kan enige tijd duren voordat klant bericht krijgt, vanwege onderzoek door SAAS leverancier)	Waarschijnlijk achteraf na detectie van aanval (kan enige tijd duren voordat klant bericht krijgt, vanwege onderzoek door SAAS leverancier)	Wordt niet via system op de hoogte gebracht, wel via procedure	1.00	0.62	0.62	kwetsbaarheden worden niet meteen gemeld aan gebruiker	T18 doubting whether providers inform them directly about detected vulnerabilities or leaks	T5 sensitive data leak	T31 No up to date insights in the amount and severity of security vulnerabilities and threats
43	3.3	Wordt er gebruik gemaakt van SLA's die ook security elementen bevatten? Welke security elementen worden in de SLA beschreven?	Het is mij niet bekend of of SLA's ook security elementen bevatten	Moet ik navragen. Google (https://cloud.google.com/security/compliance). The EU Cloud Code of Conduct (CoC) was designed to contribute to an environment of trust and transparency in the European cloud computing market and to simplify the risk assessment process of Cloud Service Providers (CSPs) for cloud customers. Security Program For Unit4 Global SaaS Operations: https://info.unit4.com/rs/300-520-631/images/U4-ALL-CLOUD-Security-Program-for-Unit4-	Beschikbaarheid, wachtwoordgebruik, etc.	1.00	0.00	0.00	SLA met security elementen worden beperkt gebruikt	T19 security elements in the SLA	T31 No up to date insights in the amount and severity of security vulnerabilities and threats	
44	3.3.1	Heeft u voorbeelden van SLA's die security elementen bevatten?	Nee, moet ik opzoeken.	Nee, moet ik opzoeken.	Niet aanwezig	0.31	0.43	0.20	Geen voorbeelden van SLA met security elementen	T19 security elements in the SLA		
45	3.3.2	Heeft u voorbeelden van SLA's die security elementen bevatten?	Nee, moet ik opzoeken.	Nee, moet ik opzoeken.	Niet aanwezig	1.00	0.20	0.20	Geen voorbeelden van SLA met security elementen	T19 security elements in the SLA		
46	4.1	Heeft u een beeld van de architectuur van de SAAS-applicatie(s)?	Gedeeltelijk	Gedeeltelijk	Gedeeltelijk	1.00	1.00	1.00	Gedeeltelijk beeld van architectuur	T20 limited picture of architecture of the SAAS applications		
47	4.1.1	Hoe zijn de componenten van de SAAS Cloud-applicatiearchitectuur met elkaar verbonden (via lokaal datacentrum of internet)?	Office 365 via internet, van de andere SAAS applicaties is dit niet bekend. In een SAAS model wordt de security gemanaged door de leverancier van de applicatie	Google Gsuite via internet (https://cloud.google.com/security/); we encrypt data in transit between our facilities and at rest, ensuring that it can only be accessed by authorized roles and services with audited access to the encryption keys.	Functioneel beheerder zou moeten weten hoe de componenten met elkaar verbonden zijn	0.38	0.68	0.11	het is niet duidelijk hoe architectuur componenten verbonden zijn	T20 limited picture of architecture of the SAAS applications		
48	4.1.2	Is de applicatie naast de gebruikelijke user interface ook via web-API-eindpunten te benaderen?	Office 365 wel, andere SAAS niet bekend.	Google Gsuite wel, andere SAAS niet bekend	Ja, er zijn applicaties die gebruik maken van API eindpunten.	0.63	0.73	0.68	er zijn applicaties via API te benaderen	T21 Multiple access possibilities	T20 limited picture of architecture of the SAAS applications	
49	4.1.3	Wat is de impact indien ongeautoriseerde apparaten zich kunnen aanmelden bij de SAAS-applicatie(s)?	Lekken van patient gegevens (datalek met alle gevolgen van dien)	Lekken van klantgegevens	Nee, aanmelden kan alleen met geautoriseerde devices (pc's, laptops, etc.)	0.48	0.61	0.30	datalek mogelijk bij gebruik niet geautoriseerde apparaten	T5 sensitive data leak		
50	4.2	Bezit de CSP certificaten voor de SAAS applicaties?	Gedeeltelijk	Gedeeltelijk	Gedeeltelijk	1.00	1.00	1.00	De CSP bezit gedeeltelijk certificaten voor de applicatie	T22 providers do have certificates	T28 not clear what kind of certificates were used	T20 limited picture of architecture of the SAAS applications

51	4.2.1	Welke certificaten zijn er?	SnelStart is ISO 9001 gecertificeerd. Microsoft is ISO/IEC 27001 gecertificeerd. <a href="https://www.microsoft.com/en-us/trustcenter/compliance/iso-iec-27001-23_self%23ISO/IEC%2027001">https://www.microsoft.com/en-us/trustcenter/compliance/iso-iec-27001-23_self%23ISO/IEC%2027001</a> . Alle SAAS applicaties gebruiken een SSL certificaat.	Google ( <a href="https://cloud.google.com/security/">https://cloud.google.com/security/</a> ). We ondergaan independent verification of our security, privacy, and compliance controls to help you meet your regulatory and policy objectives. Find details on our full set of compliance offerings, like ISO/IEC 27001/27017/27018/27701. Alle SAAS applicaties gebruiken een SSL certificaat. Unit4 (Multiverse) - TEC Certification Report: <a href="https://info.unit4.com/UA-ALL-GEN-">https://info.unit4.com/UA-ALL-GEN-</a>	PKI overheid, signed door certificaatbeheerder, en self signed zelf uitgegeven.				Gebruikte certificaten ISO, PKI, SSL	T22 providers do have certificates					
						0,37	0,65	0,40							
52	4.2.2	Worden de certificaten ook periodiek vernieuwd?	SSL certificaten jaarlijks. Microsoft services are audited at least annually against the ISO 27001:2013	SSL certificaten jaarlijks. Google cloud services are audited at least annually against the ISO 27001 standard.	Ja, afhankelijk van looptijd, gemiddeld 1 jaar	0,99	0,12	0,09	SSL certificaten jaarlijks vernieuwd	T23 security protocols were used for accessing SAAS	T22 providers do have certificates				
53	4.3	Wordt de SAAS applicatie benaderd via beveiligingsprotocollen?	Ja	Ja	Ja	1,00	1,00	1,00	applicatie wordt benaderd via beveiligingsprotocollen	T23 security protocols were used for accessing SAAS					
54	4.3.1	Welke beveiligingsprotocollen worden er gebruikt?	<a href="https://ssl">https://ssl</a>	<a href="https://ssl">https://ssl</a>	HTTPS, TLS, SSL	1,00	0,95	0,95	gebruikte protocollen https en tls	T23 security protocols were used for accessing SAAS					
55	4.3.2	Zijn deze beveiligingsprotocollen ook onderdeel van een SLA?	ja	Ja	Ja, deze zijn onderdeel van SLA	1,00	0,00	0,00	protocollen onderdeel SLA						
56	5.1	Gebruikt u ESA om de risico's van SAAS in kaart te brengen/te beheren?	Gedeeltelijk	Gedeeltelijk	Gedeeltelijk	1,00	1,00	1,00	ESA wordt beperkt gebruikt om risico's te beheren	T8 ESA is used to a very limited extent	T26 limited budget for risk management and monitoring of applications	T24 no specific role or function that is dedicated for monitoring of SAAS	T29 no ESA related governance		
58	5.1.2	Zijn er richtlijnen en principes voor implementatie van ESA?	NEN7510	Moet ik navragen, niet bekend	Weet niet	0,00	0,00	0,36	beperkt of geen richtlijnen	T8 ESA is used to a very limited extent	T29 no ESA related governance				
59	5.1.3	Beschikt de case organisatie over een service portfolio (ISMITIL), waarin risk en security zaken mbt SAAS worden meegenomen	Nee, dit wordt niet gebruikt binnen de organisatie. Er wordt helemaal geen gebruik gemaakt van een service	Moet ik navragen	Service portal is aanwezig (self-service desk) pw reset, wifiticket, etc...	0,49	0,58	0,35	Geen gebruik van service portfolio voor SAAS risk en security	T25 limited use of service portfolio (ISMITIL)	T26 limited budget for risk management and monitoring of applications	T24 no specific role or function that is dedicated for monitoring of SAAS			
60	5.2	Is er een budget voor risicobeheer en monitoring van SAAS applicaties?	gedeeltelijk	Gedeeltelijk	Gedeeltelijk	1,00	1,00	1,00	beperkt budget voor risicobeheer	T26 limited budget for risk management and monitoring of applications	T1 Small and Medium sized Enterprise	T24 no specific role or function that is dedicated for monitoring of SAAS	T29 no ESA related governance		
61	5.2.1	Zijn er medewerkers die uitsluitend belast zijn met beheer en monitoring van risk en security controls van (SAAS) applicaties?	Nee. Er is geen specifieke rol of functie die binnen onze MKB organisatie is belast met het monitoren van SAAS applicaties, dit wordt gedaan middels een reguliere rol. Een systeembeheerder doet deze werkzaamheden	Systeembeheerder doet deze werkzaamheden slechts periodiek.	CISO, security officer	0,70	0,59	0,45	geen specifieke medewerkers belast met risicobeheer	T24 no specific role or function that is dedicated for monitoring of SAAS	T1 Small and Medium sized Enterprise	T26 limited budget for risk management and monitoring of applications	T29 no ESA related governance		

Legend:

Columns	Color	Meaning
Spacy12, Spacy23, Spacy13	Red	Difference for pair comparison
Spacy12, Spacy23, Spacy13	Yellow	Low similarity for pair comparison
Spacy12, Spacy23, Spacy13	Green	High similarity for pair comparison
Similarities/Differences	Red	Difference for total of pairs
Similarities/Differences	White	Low similarity for total of pairs
Similarities/Differences	Green	High similarity for total of pairs

## Appendix G: Theme count

Theme nr	Theme	Count
T1	Small and Medium sized Enterprise	4
T2	Clear understanding of definition	3
T3	ESA goals	1
T4	policy and guidelines for access and usage of SAAS applications	4
T5	sensitive data leak	10
T6	Core business SAAS application	1
T7	Risk & security controls	1
T8	ESA is used to a very limited extent	6
T9	strict regulations for access and data storage	2
T10	subject to periodic audits	2
T11	relied on the compliance information from the certified SAAS CSP	4
T12	Privacy	1
T13	electronic authentication of humans in a SAAS application was a problem	8
T14	Available registration policy	2
T15	Availability of SAAS applications was a crucial aspect	4
T16	Availability of fail-over	1
T17	not clear if there was any ability of detection of vulnerabilities that could impact SAAS applications	2
T18	doubting whether providers inform them directly about detected vulnerabilities or leaks	1
T19	security elements in the SLA	3
T20	limited picture of architecture of the SAAS applications	4
T21	Multiple acces possibilities	1
T22	providers do have certificates	3
T23	security protocols were used for accessing SAAS	3
T24	no specific role or function that is dedicated for monitoring of SAAS	5
T25	limited use of service portfolio (ISM/ITIL)	1

T26	limited budget for risk management and monitoring of applications	6
T27	limited operational up time	1
T28	not clear what kind of certificates were used	1
T29	no ESA related governance	5
T30	limited confidence that SAAS solutions meet the requirements	1
T31	No up to date insights in the amount and severity of security vulnerabilities and threats	4



