Masters's Thesis

How to meet security standards as a cloud provider - A journey set out to clear the sky of cloud security and certifications

Jocelin Lillienau

Department of Electrical and Information Technology,
Faculty of Engineering, LTH, Lund University, 2016.

How to meet security standards as a cloud provider - A journey set out to clear the sky of cloud security and certifications

Jocelin Lillienau
ada10ili@student.lu.se

Department of Electrical and Information Technology
Lund University

Advisor: Paul Stankovski

Examiner: Thomas Johansson

February 1, 2016

Printed in Sweden
E-huset, Lund, 2016

Abstract

An upcoming trend in the current IT-landscape is to outsource services to so called Cloud Service Providers (CSPs). However, many companies are still sceptical to this new kind of services, since they bring about a certain loss of control. For this reason, it is important for CSPs to show that their services are secure. There are several options in proving this and it is up to every CSP to choose which of those options, in this report referred to as assessment schemes, that suits them best. The question is, how do they make this choice?

In the starting phase of this thesis project, an extensive information search was carried out. More than 30 different certifications, standards, attestations, ratings, assessments, reports, compliances or audits, touching upon this subject were found. Add to the equation that much of the information found was questionable or straight out incorrect, and the question of which assessment scheme to concentrate on becomes quite complex.

The described problem was identified by the Belgian company Ferranti Computer Systems, who just opened up their cloud services to customers. In collaboration with them, the following three goals were defined to solve the problem:

- Create a clear overview of the cloud assessment schemes that exist on the market
- Provide methods to categorize or compare assessment schemes
- Make a case study on Ferranti Computer Systems demonstrating how the accomplishments can be put to practice

To fulfill those goals, three main deliveries were created. First of all an overview including a short explanation of relevant assessment schemes on the market. Second, a comparison of assessment schemes in terms of risk mitigation. Four known cloud risks were put forward and some surprising observations were made. The third delivery was a case study on Ferranti Computer Systems. Previous findings in combination with results from interviews were used to select a suitable assessment scheme for their cloud platform.

The assessment scheme they chose was more or less unknown to everyone at Ferranti Computer Systems. It was the research that opened their eyes to this new assessment scheme and convinced them to try something new, rather than choosing something they knew about by reputation. Seeing how the investigation changed

their mind, it became obvious how important it is to create more transparency in the world of assessment schemes. It is essential that companies choose the assessment scheme that is most suitable for them and that they have a clear understanding of why it is suitable. This thesis proves the need for clarity among cloud security assessment schemes and presents methods to achieve this clarity.

Foreword

This thesis was carried out as a part of a Master of Computer Science and Engineering at Lund Univeristy, faculty of engineering, LTH. A big thank you to Paul Stankovski, assistant senior lecturer at LTH, who has been a very committed and helpful mentor in every part of the process.

The thesis was executed in collaboration with the Belgian company Ferranti Computer Systems, situated in Antwerp. I would like to send my gratitude to them for offering me this project and guidance along the way. A special thank you to Rafael De Backer, Enterprise Architect at Ferranti ICT, who has been a great mentor, participant and reviewer throughout the whole project.

Further, I wish to say a big thank you to Peter Lesage, my private sound board and reviewer, who is always full of great ideas and suggestions for improvements.

Last, I would like to thank my Irish friends Gary Flynn and Beatrice Gates-Hardiman that, as native English speakers, have assisted me with the grammar.

Table of Contents

Abbreviations

- AT - Attestation Standard
- CAIQ - Consensus Assessments Initiative Questionnaire
- CCM - Cloud Controls Matrix
- CCSM - Cloud Certification Schemes Metaframework
- CIF - Cloud Industry Forum
- CSA - Cloud Security Alliance
- CSP - Cloud Service Provider
- DSS - Data Security Standard
- ECSA - EuroCloud Star Audit
- ENISA - European Union Agency for Network and Information Security
- HIPAA - Health Insurance Portability and Accountability Act
- HITECH - Health Information Technology for Economic and Clinical Health
- ICT - Information and Communications Technology
- ISAE - International Standard on Assurance Engagements
- ISMS – Information Security Management System
- ISO – International Organization for Standardization
- ITIL – Information Technology Infrastructure Library
- OCF - Open Certification Framework
- P2PE - Point-to-Point Encryption
- PA-DSS - Payment Application Data Security Standard
- PCI - Payment Card Industry
- PHI - Protected Health Information
- PTS - PIN Transaction Security

- RFP - Request For Proposal
- SAS - Statement of Auditing Standard
- SMS – Service Management System
- SOC - Service Organization Control
- SSAE - Statement on Standards for Attestation Engagements
- SSC - Security Standards Council
- QMS – Quality Management System

List of Figures

List of Tables

Chapter 1
Introduction

When talking about the unstoppable trend of cloud computing the first thing that crosses many peoples mind is, "Is it really hundred percent reliable?" The doubt lies in many different factors such as the quality of providers, the loss of control but maybe most of all in the security assurance. Is the data actually safe, can I be sure that it will not be lost and that outsiders will not be able to access it? Obviously, no person or company can actually assure this to the full extent. New threats are arising every day and so far the inventors of threat mitigation are behind in the race against the inventors of the threats. However, something that can be assured, or proved, is that a certain cloud service is as safe as it can be from a work-practical perspective, considering the threats we know about today.

There are several options in proving this and it is up to every Cloud Service Provider (CSP) to choose which of those options that suits them best. The question is, how do they make this choice? What makes one option more suitable than another? And how do you actually reach or live up to your desired assessment scheme, meaning certification, standard, attestation, rating, assessment, report, compliance or audit?

In the following chapters, you can read about how this thesis project helped an upcoming CSP on their journey.

1.1 Background

The project was carried out at the Belgian company Ferranti Computer Systems, which in the rest of this publication will be referred to as Ferranti. Their main business is to deliver software and hardware solutions to customers' private infrastructure. These customers are more and more looking for a full service, where they are no longer dependent on local infrastructure. Ferranti has therefore developed a private cloud solution that provides their clients with all required capabilities.

When selling cloud solutions as a service an important aspect is to show that the service is secure. A common way of proving this is to adopt an assessment scheme. However, on the market today, many different assessment schemes can be found. This makes it hard for CSPs to know which ones to pick. The process of implementing assessment schemes is, most of the time, quite cost and resource consuming. For this reason it is important that companies know which assessment schemes to focus on. Additionally they have to be able to make a plan on how to

acquire and maintain the chosen ones.

1.2 Problem Definition and Project Goals

As mentioned in the background section above, there is an abundance of assessment schemes on the market. Most of them have a unique focus but they often overlap in one way or another. First of all it is hard to know which assessment schemes that exists. Second, it is not clear for which purpose they are designed or what they actually assure. Third, it is close to impossible to know which overlaps that exists among them.

Of those reasons every CSP that wants to reach certification or similar target will have to start with unveiling the mystery around which assessment scheme to engage in. A big threshold is hereby created and many CSPs are forced to hire consultancy to even understand the basics. The question is, is it really this complicated? Maybe relevant assessment schemes could be assembled and presented in plain English? Maybe there is a way to compare or categorize them?

Every CSP is special. Services are designed in various ways, customers reside in different parts of the world and both have individual needs or motivations. To define an assessment scheme process that fits every single CSP is therefore impossible. However, there must be a way to make the process more transparent.

Striving towards this ambition, the current thesis has three main goals:

- Create a clear overview of the cloud assessment schemes that exists on the market
- Provide methods to categorize or compare assessment schemes
- Make a case study on Ferranti demonstrating how the accomplishments can be put to practice

Chapter 2
Methodology

To begin with, an extensive information search was carried out, to see which assessment schemes that were available on the market. The relevant ones were collected in an overview, which can be found in Chapter 3. Once this overview was finished, ways to compare the assessment schemes was investigated. It is commonly known that a big problem with cloud services is security assurance, therefore the decision was made to make a comparison in terms of risk mitigation. This comparison can be found in Chapter 4.

In the next step, focus was put on Ferranti, where employees and internal customers were interviewed. Partly to find more ways of comparing the assessment schemes but also, more importantly, to see which of them that could be a good option for Ferranti. With the result from the interviews as a base, tables and charts were created. Using these, a filtering was performed, which resulted in three different alternatives. The final choice of which assessment scheme to pick was put in the hands of people from Ferranti. To facilitate them in making this decision, a SWOT analysis for each of the remaining options was created. Assisted by those, the involved people came to an agreement and an assessment scheme was selected. Information regarding the interviews can be found in Chapter 5 while an ingoing description of the filtering can be found in Chapter 6.

2.1 Applied methods in the thesis

2.1.1 SWOT

During a SWOT analysis an organization compares its own capabilities, in terms of strength and weaknesses, with the external environment, in terms of opportunities and threats. They want to investigate how future developments and influences coming from outside the organization can form a challenge to their current business processes and models. Based on this insight they can make better decisions on how to tackle these factors. The illustration in Figure 2.1 serves as an example of how a SWOT is usually made.

Table 2.1: Example of a SWOT diagram

The SWOT model in this thesis placed three assessment schemes as the central point of attention. For each one of them a closer look was taken at what their strengths and weaknesses were to compare them to what opportunities and threats they formed from Ferranti's perspective.

Chapter 3

Cloud Assessment Schemes Overview

An overview of assessment schemes relevant to CSPs. As an aid to the reader, a list of presented assessment schemes can be found below.

3.1 Service Organization Control (SOC) framework

Statement of Auditing Standard (SAS) 70 was a recognized standard used in third-party auditing for service organizations. The original focus of this standard was financial reporting. However, it got stretched over the years to also cover assurance of other types of controls, such as managed security services and data center co-location services [1].

SAS 70 was on June 15th 2011 effectively replaced by Statement on Standards for Attestation Engagements (SSAE) 16 for use in the U.S. and International Standard on Assurance Engagements (ISAE) 3402 for global use [2]. The two of them are very similar but have a few differences, which can be found in [3]. These two standards are focused solely on controls regarding financial reporting. When carrying out an auditing regarding any of those two standards, you will receive a so called SOC 1 report. This will state the efficiency and accuracy of which the controls are fulfilled within the service organization. There are two different types of SOC 1 reports, type I and type II. The difference between the two is that type I only refers to a certain point in time while type II refers to a *period* of time [4].

An audit regarding other matters than financial reporting, will instead be made according to the standards Attestation Standard (AT) 101, for use in U.S. and ISAE 3000, for global use [1][5]. The controls in these standards are typically related to IT and evaluates a service organization's information systems with respect to security, availability, processing integrity, confidentiality or privacy [6][4].

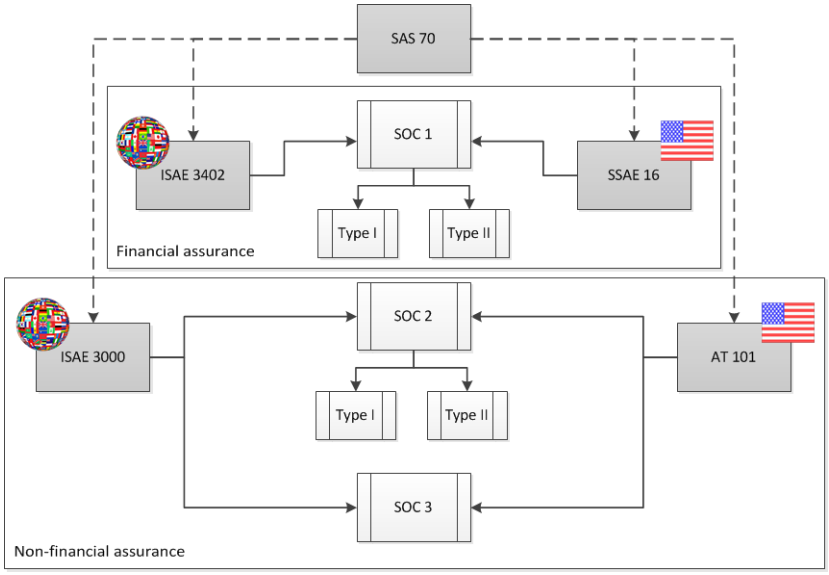

Figure 3.1: Visual overview of the SOC framework

An audit of any of those two standards can result in either a SOC 2 report or a SOC 3 report. The choice of which one to acquire is made by the service organization. The difference between them is that SOC 2 is made for internal use and SOC 3 is made for public use. This means that a SOC 2 report carries highly

technical details and sometimes secret information, while a SOC 3 report is more general and carries only information that can be used for marketing. The more detailed SOC 2 can, just as SOC 1, be acquired in type I or type II [4].

Something very important to note when talking about SOC reporting framework is that just because you have gone through an audit regarding one of the mentioned standards and received a SOC report, it does not mean that you hold any kind of certification. The only thing you have is a report on compliance status [7][8].

A visual overview of the SOC framework can be seen in Figure 3.1.

3.2 ISO standards for CSPs

The International Organization for Standardization (ISO) has released an uncountable number of standards over the years. This cloud assessment schemes overview presents the ones considered valuable to CSPs, namely the ISO 9000 family of Quality Management System (QMS) standards, the ISO 27000 family of Information Security Management System (ISMS) standards, the ISO 20000 family for Service Management System (SMS) standards as well as the two standalone cloud computing standards ISO 17788:2014 and ISO 17789:2014. Figure 3.2 shows an overview of those standards and which ones that allow for official certification.

3.2.1 ISO 9000 series for QMS

The ISO 9000 series is probably the most widely known standard series published by the ISO [9]. It can be implemented by all kinds of organizations and ensure quality in organizations' processes and products [10]. The series consists of four standards. Firstly ISO 9001:2015, which is the only standard in the series that you can become certified against. The reason for this, is that it defines the actual requirements of a QMS [11]. Then there is the ISO 9000:2005, which explains the overall concept of the series as well as the terms and vocabulary being used [12]. For sustained success on a long-term basis, there is the ISO 9004:2009 [13]. This standard goes beyond ISO 9001:2015 and provides guidance on how to further improve general performance [12]. Lastly, there is the ISO 19011:2011 (earlier referred to as ISO 10011), which offers guidance on audits of quality management systems [14].

3.2.2 ISO 27000 series for ISMS

ISO 27001:2013 is a list of requirements that need to be fulfilled to achieve an ISO 27001:2013 certified ISMS. A portion of those requirements goes into the details of information security risk treatment. A part of this portion is to go over a pre-defined list of controls and make sure all necessary controls have been implemented. The pre-defined list can be found in Annex A of the ISO 27001:2013 standard. There you can find a short description of every control, about one sentence long. If you then look in the ISO 27002:2013 standard you will find the same list of controls, even with the same numbering. However, here the one sentence describing the control will also be followed by implementation guidance

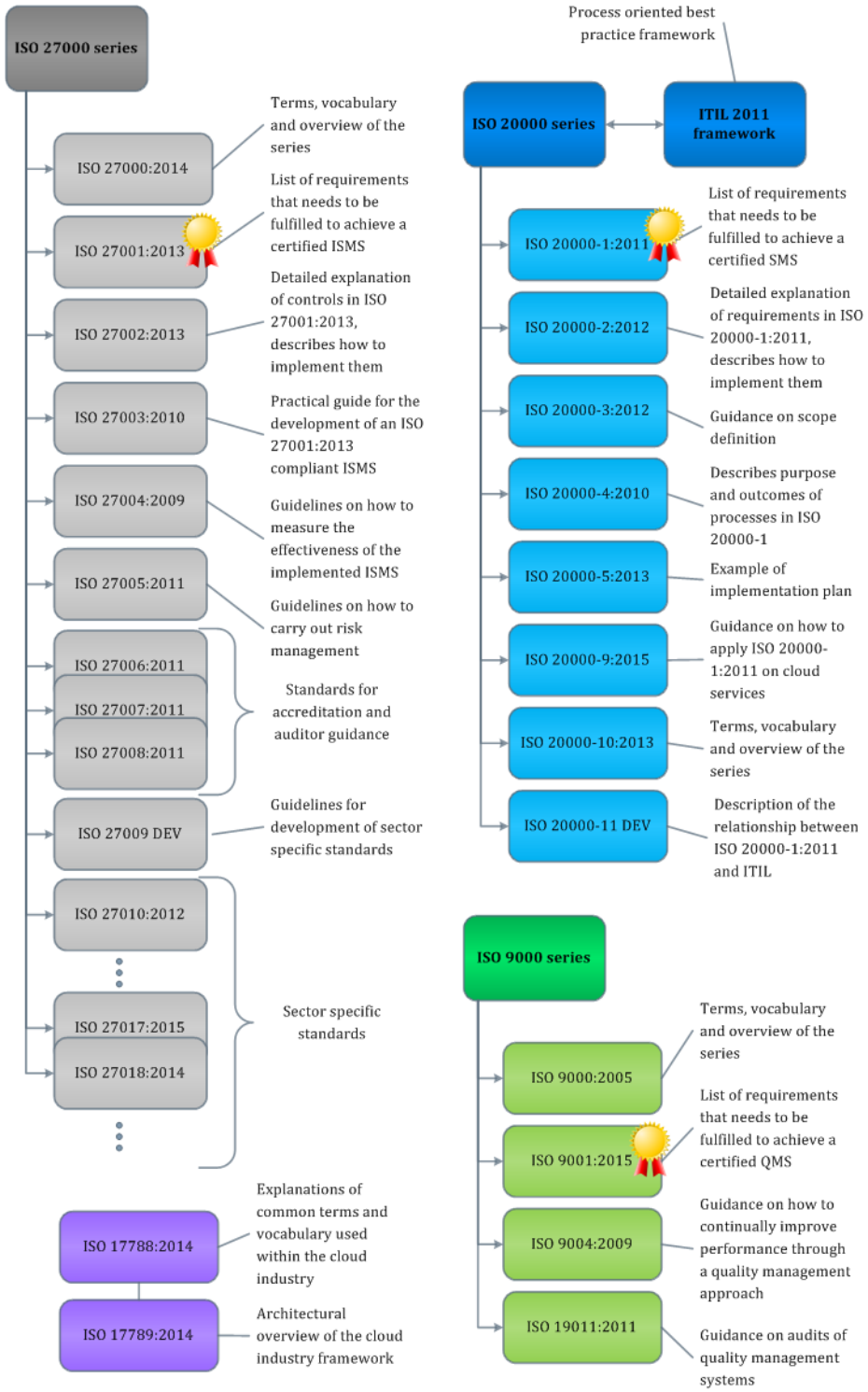

Figure 3.2: Graphical overview of ISO standards relevant to CSPs

and other information regarding the control. All in all ending up with about one page per control [15].

Important to note is that ISO 27002:2013 does not include any sort of requirements, which is why you cannot become certified against it. However, an audit firm, with good enough knowledge on the subject, can make an informal review or audit against ISO 27002:2013. By going through one of those you can show that you have your security model under control even though you have not achieved an ISO 27001:2013 certification [16][17][18][19].

ISO 27001:2013 is the only standard within the 27k series that you can achieve an official certification against. The rest of the standards offer guidance on a certain subject and are to be used as a complement to the ISO 27001:2013 standard [15][20][21]. The subject of some standards in the ISO 27000 series can be seen in Figure 3.2. Looking at the sector specific standards there is one named ISO 27018:2014 and one named ISO 27017:2015. These two standards are both connected to cloud security and shall be used for guidance on how to implement controls from ISO 27001:2014 in a cloud computing setting. They can be seen as an extension of 27002:2013 and just as with this standard, an informal review or audit against them can be carried out. However, an official certification against them is not possible [22].

3.2.3 ISO 20000 series for SMS

ISO 20000 has a different way of numbering the standards than the ISO 9000 and ISO 27000 series. However, it can still be referred to as a series and the different parts of ISO 20000 are still comparable with the different standards in the ISO 27000 and ISO 9000 series. There is a standard that lists terms and vocabulary for the series, however here it is named ISO 20000-10:2013. ISO 20000-1:2011 is just as ISO 9001:2015 and ISO 27001:2013, a list of requirements that needs to be fulfilled to reach certification. ISO 20000-2:2012 is a code of practice, which gives more ingoing information about each requirement in ISO 20000-1:2011, including information on how to implement them [23].

ISO 20000-3:2012 gives guidance on scope definition, which is of great help when applying ISO 20000 series on a bigger organization. ISO 20000-4:2010 is supposed to describe each process in ISO 20000-1, in terms of purpose and outcomes. However, ISO 20000-4:2010 is outdated and not aligned to ISO 20000-1:2011 [24][23]. ISO 20000-5:2013 gives an example of an implementation plan for ISO 20000 series with hints and templates [23][25]. The newest standard in the series is the ISO 20000-9:2015, which provides guidance for organizations that want to apply ISO 20000-1:2011 on cloud services [26].

ITIL 2011 framework

Next to the ISO 20000 series there is Information Technology Infrastructure Library (ITIL) 2011. This is not a standard but a best practice library with focus on operational processes. It gives you advice on how you can implement processes but it does not say that you have to do it according to this advice [27]. It is similar to ISO 20000-2:2012 but does not have a direct connection to each requirement in

ISO 20000-1:2011. It also has a wider and deeper scope, meaning it covers more processes and gives more in-depth knowledge about how to implement them [28].

It is advised to implement ITIL in combination with the ISO 20000 series. ITIL will be of great help in understanding the details of the processes needed to be implemented to reach ISO 20000-1:2011 certification [28]. Furthermore, there is at the time of writing a standard called ISO 20000-11 being developed, which will lay out the relationship between the ISO 20000 series and ITIL [23].

3.2.4 Other ISO standards related to cloud computing

Except for the ISO series mentioned above there are two more ISO standards with value to CSPs, namely ISO 17788:2014 and ISO 17789:2014. These standards do not contain any requirements, meaning you cannot get certified against them. They simply explain the basic terminology and architectural framework of the cloud industry [29].

3.3 CSA Open Certification Framework (OCF)

Cloud Security Alliance (CSA) OCF combines well known standards from the market with tools from CSA, in an attempt to make a globally accepted, easy to work with framework for security recognition of CSPs. It consists of three levels, namely self-assessment, third-party assessment-based certification and continuous monitoring-based certification [30][31]. Figure 3.3 shows an illustration of the three levels.

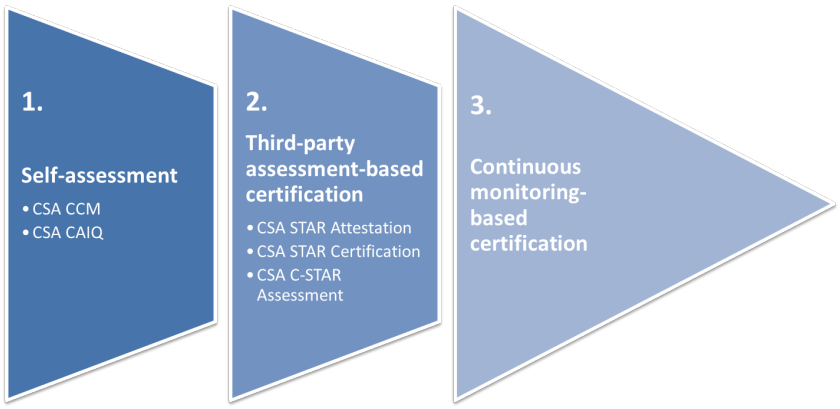

Figure 3.3: Illustration of the CSA OCF

At the first and basic level, the CSP makes a self-assessment using either the CSA Cloud Controls Matrix (CCM) [32] or the CSA Consensus Assessments Initiative Questionnaire (CAIQ) [33]. The CSP can submit the report from the self-assessment to the CSA, they will then make sure it becomes publicly available [34].

The second level holds three different alternatives of third-party assessment. CSA STAR Attestation, which is a combination of SOC 2 and CSA CCM and

CSA STAR Certification, which is a combination of ISO 27001:2013 and CSA CCM. Important to note, is that the CSA STAR Attestation results in a report on compliance, while the CSA STAR certification results in a certification [35]. Lastly, there is also the CSA C-STAR Assessment, which is specialized on the Chinese market and therefore combines CSA best practises with Chinese national standards [31].

The third level is still under development but will be built on CSA best practices and handle continuous auditing and assessment [36].

3.4 EuroCloud Star Audit (ECSA)

The ECSA is an assessment schemes focused solely on certification of cloud services. Just as with the CSA Open Framework, the first step in getting certified is to perform a self-assessment. In ECSA's case this is done through their online assessment tool. The result of this self-assessment can be published on the website of ECSA but demonstrates only what a certain CSP thinks of themselves. To acquire an official ECSA certification the CSP must go through an official audit carried out by an ECSA accredited auditor organization [37][38][39].

3.5 TÜV Rheinland Cloud Security Certification

TÜV Rheinland is a technical service provider, offering solutions globally within safety and certification. One of the certifications they are offering is the TÜV Rheinland Cloud Security Certification. The requirement catalogue of the certification is based on studies, regulations and recommendations as well as standards such as ISO 27001. The company is based in Germany, where it is currently also the most recognized independent inspection authority. Certificates can only be issued directly by TÜV Rheinland [41][42].

3.6 PCI security standards

The standards from the Payment Card Industry (PCI) Security Standards Council (SSC) focus mainly on payment card data security. The most common of these standards is PCI Data Security Standard (DSS) which is very important for all merchants, or service providers, that handle any sort of cardholder data. It provides processes for everything from prevention and detection to mitigation and treating of security incidents.

Apart from this key standard PCI SSC also provides three more standards. PCI PIN Transaction Security (PTS), which holds a list of requirements for PIN terminals. PCI Payment Application Data Security Standard (PA-DSS), which can be used for approval of payment applications. PCI Point-to-Point Encryption (P2PE), which offers a list of requirements covering the whole framework and ensures a safe P2PE solution [40]. It is easy to see how the standards from PCI SSC are connected in Figure 3.4.

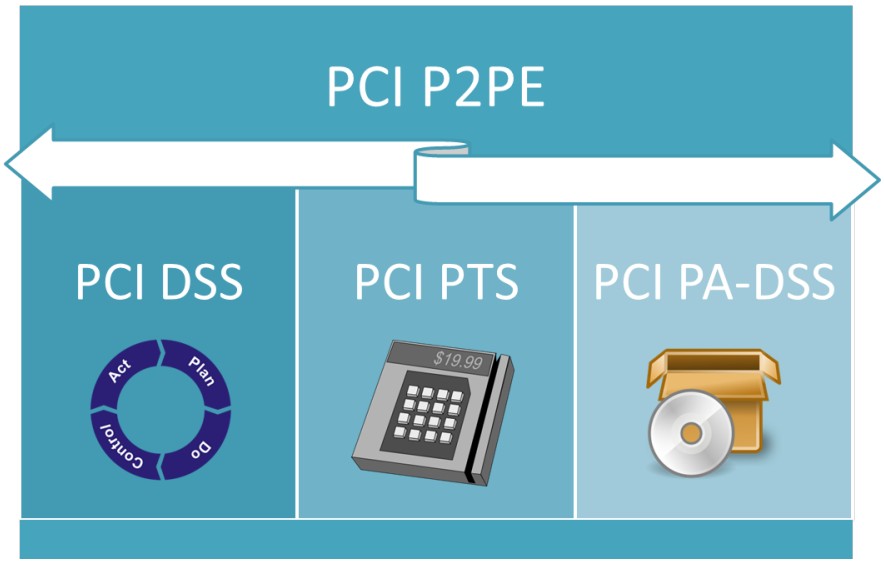

Figure 3.4: Graphical representation of PCI security standards

3.7 LEET Security Rating

LEET Security is a rating agency for Information and Communications Technology (ICT) Services, the first one of it's kind in Europe. They are based in Spain, where they have been operating since their start in 2010. They rate all sorts of services offered by ICT service providers and are specialized on information security in cloud environments [44]. Worth noticing is that they do not certify the providers as a whole, they rate only their individual services. This means that the same provider can have different ratings on their different services.

A rating is split up in three dimensions, Confidentiality, Integrity and Availability and based on a list of controls. Each of these dimensions will be appointed to a grade ranging from A to E, where A is the best score. A service rating is thereby made up by a three-letter combination, where any of these letters can be changed based on follow up activities. Follow up is performed through random audits, feedback from the users of the service as well as obliged reporting from service provider when changes, that can effect the rating, are made. As with star ratings of hotel chains, the service provider decides themselves which level of rating that they want to achieve. An audit is then performed by LEET security and certification, with the desired letter combination, will be granted if the controls required for this rating are in place.

In addition to the three letters a star (*) or a plus (+), can be added to the rating. The star means that the service is also compliant with version 2.0 of the PCI DSS standard and the plus means that the service is also compliant with the Spanish privacy Law 15/1999 and regulatory development, RD 1.720/2007. Those symbols are added to the letter representing the confidentiality dimension, which is also the dimension they are applicable to [45].

3.8 CIF Self-Certification

Cloud Industry Forum (CIF) is a membership-based not-for-profit organization situated in the United Kingdom. It was created by a couple of organizations, from the cloud industry, to solve the problem of lack of transparency and trust in cloud services. They wanted it to become easier for cloud service customers to compare CSPs and to trust cloud services in the same way they trust traditional services [46].

Their solution to this problem was to create a code of practice for CSPs. This code of practice consists of guidelines and best practices on how to provide good quality services in the cloud [47]. CSPs can certify themselves against this code of practice through a self-certification process [48]. Since it is a self certification, this is done with an organizations own resources. Detailed instructions of the procedure can be found on the website of CIF. However, to keep the code of practice up to date and to keep the organization going, a small certification fee is taken out by CIF on a yearly basis. This fee is dependent on the CSPs turnover and is ranging from £200 to £3500 [46].

Once the self-certification process is finished the CSP is allowed to use the certification logo of CIF and will be listed on the website of CIF. To keep the logo and the spot in the list, a yearly self-certifications is required. In a similar way as LEET security, CIF will carry out random checks of conformity as well as listen in on complaints regarding non-compliance [49].

3.9 HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) is part of the U.S. legislation. It is subdivided into five titles, covering different areas of the safekeeping of protected health information (PHI). The second one of those titles, HIPAA Title II, provides standards connected to electronic access to and electronic transaction of health information [50]. Certification against those standards is not possible. However, every organization that is active in the U.S. market and handles PHI has to make sure they are compliant [51][52]. The determination of whether an organization is compliant is up to themselves to make. Important to note is, however, that failure to comply counts as violating the U.S. law and can result in serious consequences [53].

3.9.1 HITECH

The Health Information Technology for Economic and Clinical Health (HITECH) Act is an extension to HIPAA that was created to support the adoption and meaningful use of electronic health records (EHR) and other health information technology [54][55].

Chapter 4

Comparison in terms of Risk Mitigation

When comparing assessment schemes, an important aspect is security and risk mitigation. Therefore, a comparison was performed, disclosing which counteractions to risks that are assured in the different assessment schemes. The choice of which risks and counteractions to include is based on knowledge gained from web and computer security courses at Lund University as well as the article "The 5 cloud risks you have to stop ignoring" by Roger A. Grimes [56].

In the analysis the Cloud Certification Schemes Metaframework (CCSM) [57], created by The European Union Agency for Network and Information Security (ENISA), was used. This is a framework that includes most of the assessment schemes in the overview. It has a list of predefined security objectives with short descriptions. When choosing one or more of those security objectives, it produces a matrix showing which of the assessment schemes that have addressed the chosen security objectives. Worth noticing is that what in this report is refereed to as an assessment scheme is in the CCSM referred to as a certification scheme. However, the two words have the same meaning.

Counteractions to some of the defined risks could be found among those security objectives and this was used as a base in the comparison. In case a risk was not fully addressed by the security objectives in the CCSM, documentation about the assessment schemes was analyzed to see whether the risk was specifically addresses or not. The security objectives that were used can be found in Table 4.1.

The CCSM includes the following assessment schemes:

- SOC 2 report
- SOC 3 report
- ISO 27001 Certification
- CSA Self Assessment
- CSA STAR Attestation
- CSA STAR Certification
- EuroCloud Star Audit

- EuroCloud Self Assessment
- TÜV Rheinland Cloud Security Certification
- LEET Security Rating
- CIF Self-Certification

The rest of the assessment schemes in the overview were excluded from this part of the investigation.

CCSM Security Objective	**Description**
1. Information security policy	Cloud provider establishes and maintains an information security policy
6. Security knowledge and training	Cloud provider verifies and ensures that personnel have sufficient security knowledge and that they are provided with regular security training
7. Personnel changes	Cloud provider establishes and maintains an appropriate process for managing changes in personnel or changes in their roles and responsibilities
9. Security of supporting utilities	Cloud provider establishes and maintains appropriate security of supporting utilities (electricity, fuel, etc.)
10. Access control to network and information systems	Cloud provider establishes and maintains appropriate policies and measures for access to cloud resources
11. Integrity of network and information systems	Cloud provider establishes and maintains the integrity of its own network, platforms and services and protect from viruses, code injections and other malware that can alter the functionality of the systems
14. Asset management	Cloud provider establishes and maintains asset management procedures and configuration controls for key network and information systems
18. Disaster recovery capabilities	Cloud provider establishes and maintains an appropriate disaster recovery capability for restoring cloud services provided in case of natural and/or major disasters
19. Monitoring and logging policies	Cloud provider establishes and maintains systems for monitoring and logging of cloud services
22. Checking compliance	Cloud provider establishes and maintains a policy for checking compliance to policies and legal requirements
23. Cloud data security	Cloud provider establishes and maintains appropriate mechanisms for the protection of the customer data in the cloud service

Table 4.1: CCSM Security Objectives used in the comparison

4.1 Known Risks and Counteractions

4.1.1 Access by unauthorized users

To avoid the risk of unauthorized users getting access to the cloud platform, strong authentication is crucial. This involves user credentials being stored safely and kept up to date. Only the most vital users should have access and these people should be well educated in how to treat their credentials.

Mitigation to this risk can be found in the CCSM, embodied by three different security objectives. 6 and 10, which both turned out to be addressed by all the assessment schemes in the CCSM. Additionally 7, which is addressed by all assessment schemes except EuroCloud Self Assessment.

4.1.2 Several customers on the same platform

A CSP will host several customers on the same platform, which means that they will share resources. This comes with the risk that the customers might find out about each other or even be able to reach each others data. To overcome this risk it's important that the infrastructure of the CSP offers a strictly divided and isolated environment for each customer.

In the CCSM, there are two security objectives that touch upon this subject, namely 23 and 10. Security objective 23 should ensure that one customer's data is separated from other customers data. However, segregation on platform level is hard to achieve and requires that you set up an infrastructure per customer with virtualization techniques. By doing this, customer isolation can be achieved to a certain level but hardware devices are still, in practise, shared by multiple customers. Therefore, security objective 10 will also be of great help in supporting the segregation of customers' infrastructures. As earlier mentioned, is security objective 10 being addressed by all the assessment schemes in the CCSM. Considering then security objective 23, this is addressed by all except the ISO 27001 certification.

However, important to note is that these two security objectives are still quite general and do not provide a hard guarantee of isolation between customers. To find out which ones of the assessment schemes that offers this, the documentation of each one of them were analyzed. The conclusion is that the following assessment schemes are addressing the matter of separation between customers directly, the rest are not.

- CSA Self Assessment
- CSA STAR Attestation
- CSA STAR Certification
- TÜV Rheinland Cloud Security Certification
- LEET Security Rating

4.1.3 Deviating IT-security policy

There is a risk that the CSP and its services does not live up to the IT-security policies of the cloud customer. Some customers have strict regulations regarding where and how they can store data, how it is being processed, what it is being used for and so on. For these customers it is of greatest importance that the CSP is complying to necessary policies and legal requirements and that they have procedures to keep them updated.

Of course, there can be very specific regulations for specific businesses, but in the general case this risk is covered by security objectives 1 and 22. These two security objectives have both been addressed in all the assessment schemes in the CCSM.

4.1.4 Inaccessible data

When storing data in the cloud there is a risk that it is not always available. This can be due to system failure or simply a lack of Internet access. There is also the worse case when the data disappears entirely due to malicious attacks or other types of hazards. To avoid this you have to make sure that your CSP is offering high availability, excellent backup systems and disaster recovery solutions.

In the CCSM there are five security objectives that represents the most important building blocks in mitigating this risk. First of all 18 and 11, which speaks for themselves. To take into account the physical part of the CSP solution there is 9, which certainly is a vital part of offering high availability. Here is also 14 of greatest importance. This security objective makes sure that the CSP has a contingency plan for ensuring that vital parts of their system gets replaced due to end-of-life or breakdown. Last but not least 19 was included, which gives a proof of statements such as guaranteed up-time or successful backups.

With these security objectives you will have a solid base, it is however important to note that every system is different and that further, more specific assurance may be needed to guarantee that your data is always available.

Most of these security objectives have been addressed in most of the assessment schemes. The exceptions are EuroCloud self-assessment, which has not addressed 9 or 14, and CIF self-certification, which has not addressed 19 or 14.

4.2 Matrix Comparison

The matrix in Table 4.2 summarizes the findings. It shows the assessment schemes as rows and the cloud risks as columns. In case an assessment scheme did not address all aspects of a risk, the option partly addressed was chosen.

	Access by unauthorized users	Several customers on the same platform	Deviating IT-security policy	Inaccessible data
CIF Self Cert.	✓	~	✓	~
CSA Self Assesm.	✓	✓	✓	✓
CSA STAR Attest.	✓	✓	✓	✓
CSA STAR Cert.	✓	✓	✓	✓
EuroCloud Self Assessm.	~	✓	✓	~
EuroCloud Star Audit	✓	~	✓	✓
ISO 27001 Cert.	✓	~	✓	✓
LEET Security rating	✓	✓	✓	✓
SOC 2 Report	✓	~	✓	✓
SOC 3 Report	✓	~	✓	✓
TÜV Rheinland Cloud Sec. Cert.	✓	✓	✓	✓

✓	Fully addressed
~	Partly addressed

Table 4.2: Known cloud risks addressed per assessment scheme

Chapter 5

Interviews to Identify Key Characteristics

5.1 Who Was Interviewed?

When making a decision about which assessment scheme a company should try to attain, it is important to get a clear understanding about the goals and expectations of this project. This can be achieved by a 360 degree activity, in which you gather opinions from several various perspectives. Therefore, people with different functions in the company were interviewed:

- Stijn Verhoeven, System Architect. Responsible for the design of Ferranti's cloud solution.
- Martina Vroblova, Quality and Business Process Manager at Ferranti, meaning she handles certifications and audits within this subject.
- Johan Vandekerckhoeve, product manager of Ferranti's internal customer MECOMS. Knows what sort of requests and concerns that are coming in from MECOMS customers.
- Rafael De Backer, Enterprise Architect at Ferranti ICT. Has a close eye on the long term strategy for the cloud platform as well as a clear understanding of the underlying infrastructure.

5.2 Analysis of Interviews

Early in the interview process it was observed that when you ask people which assessment schemes they find important, they will mention the ones that they have a notion about or that they know about by reputation. In an attempt to widening the view of the interviewees, the cloud assessment schemes overview (Chapter 3) was sent out to them on beforehand. Still, most of them answered with the probably most known one, ISO 27001, when getting the direct question of which assessment scheme they thought would be most important to acquire for Ferranti's cloud platform. Maybe it is this simple, maybe you should just go for the one that is most known. In this way you can use your assessment scheme for marketing and effectively show customers that you are doing things according to best practices.

However, a closer look at the assessment schemes and the comparison of them, will make one realize that it is not this simple. The recognition is certainly an

essential factor when choosing assessment scheme but one will see that there are also other important factors that needs to be taken into account. In the analysis of the interviews it was therefore examined what the interviewees thought were the most important characteristics in a good assessment scheme, rather than which assessment scheme they named. Table 5.1 contains those characteristics and displays how they are realized in the different assessment schemes. This table also holds some columns that are not directly connected to the interviews but that were still considered meaningful to include.

Certification/Standard	Type	Current operational area	Applicability	Acknowlegding party	Target
CIF Self Cert.	Self Assessment	World wide	Cloud providers	Accredited 3rd party	Both
CSA Self Assesm.	Self Assessment	World wide	Cloud providers	Applying organisation	Both
CSA STAR Attest.	Compliance	World wide	Cloud providers	Accredited 3rd party	Both
CSA STAR Cert.	Certification	World wide	Cloud providers	Accredited 3rd party	Both
EuroCloud Self Assessm.	Self Assessment	World wide	Cloud providers	Applying organisation	Both
EuroCloud Star Audit	Certification	World wide	Cloud providers	Accredited 3rd party	Both
HIPAA	Self Assessment	USA	Health industry	Applying organisation	Organizations
ISO 20000 Cert.	Certification	World wide	IT service providers	Accredited 3rd party	Organizations
ISO 27001 Cert.	Certification	World wide	All kinds of organizations	Accredited 3rd party	Both
ISO 9001 Cert.	Certification	World wide	All kinds of organizations	Accredited 3rd party	Organizations
LEET Security rating	Other	Spain	ICT service providers (mainly cloud)	Governing organisation	Services
PCI DSS	Compliance	World wide	Payment card industry	Governing organisation	Organizations
SOC 2 Report	Compliance	World wide	Service providers	Accredited 3rd party	Both
SOC 3 Report	Compliance	World wide	Service providers	Accredited 3rd party	Both
TÜV Rheinland Cloud Sec. Cert.	Certification	Europe	Cloud providers	Governing organisation	Services

Table 5.1: Key characteristics of the assessment schemes

5.3 Key Points from Interviews

Many helpful opinions came up during the interviews, below they are summarized in a number of key points.

5.3.1 Preferably internationally recognized

In some of the interviews it came up that even if Ferranti for the moment is operating mostly in Europe, there are future plans of going to America and Asia. To be prepared for this, the assessment scheme they decide to go for should be internationally recognized. For this reason a column was included, in Table 5.1, listing the current operational area for the different assessment schemes.

5.3.2 The quality of the acknowledging party is essential

As an expert on certifications and audits, the Quality and Business Process Manager at Ferranti took up the importance of having a good notified body or acknowledging party. It should be one with quality auditor skills and a pragmatic approach focused on business risks. Her opinion was that this would make it easier to sell the added value to management. Obviously it is hard to map the auditor skills offered on a personal level but at least a column, showing who is carrying out the audit and acknowledging the proof of conformity, was introduced.

5.3.3 Customers concerns should be in the center

All of the interviewees put forward the fact that one of the biggest reasons to attain an official recognition of security is the customers. They are looking at assessment schemes mostly because customers request it. The question is then, what is the underlying expectation or motivation of the customers when requesting a certification or similar official recognition of security? One of the interviewees expressed that many customers are skeptical to the cloud and often show up with a long list of requirements that needs to be fulfilled by the provider. To go through those lists takes a lot of time, so something that could really make the tender process more efficient, would be to work with an assessment scheme with a wide scope. In this way the simple answer to many of those requirements could be just a reference to controls or processes in this assessment scheme. Moreover, there will be no discussion about the value of the solution provided. For this reason, a category called Applicability was included in Table 5.1. Herein, it was noted down what sort of organization the assessment scheme is aiming at. In this way one can at least see which assessment schemes that have a too narrow or inaccurate scope.

5.3.4 Risk mitigation is a must

Apart from the importance of following customers' requests, a couple of the interviewees also mentioned risk mitigation as a main reason to attain an official recognition of security. It is important to get to know the risks connected to cloud computing and how to mitigate them. This so you can promise safety to management and customers, by for example making sure malicious attackers can not harm the system. A comparison regarding risks and counteractions addressed in most of the assessment schemes was made in Chapter 4. Hence, this could be used instead of putting a column for risk mitigation in Table 5.1.

5.3.5 Recognition is an important factor

Even if you can not, as mentioned above, rely solely on the recognition of an assessment scheme, of course it is still an important part. As mentioned by some of the interviewees, certainly from a marketing perspective. It is something that people know and trust, even if they do not exactly know what it actually assures. Secondly as the Enterprise Architect at Ferranti ICT mentioned, you do not want to be the early adapter of an assessment scheme. The bigger, more known players, usually have several versions and revision behind their assessment schemes, which of course makes it more reliable.

The question is then, how do you measure how known, recognized or developed an assessment scheme is. This is certainly a quite substantial task and will of course be dependent on the target group you pick. In this case the task has been simplified by limitation of the target group to consisting solely of customers and employees of Ferranti. It was performed by asking the interviewees which assessment schemes they had heard of before and by looking at samples of customers' requests for proposals (RFP).

Chapter 6

Selection of an Appropriate Assessment Scheme

6.1 Filtering of the Assessment Schemes

To make it easy to filter the assessment schemes based on the characteristics in Table 5.1, a pivot chart was created. In this chart desired characteristics could be selected and unwanted ones could be deselected. Figure 6.1 is showing the start mode of the pivot chart, with all the assessment schemes included.

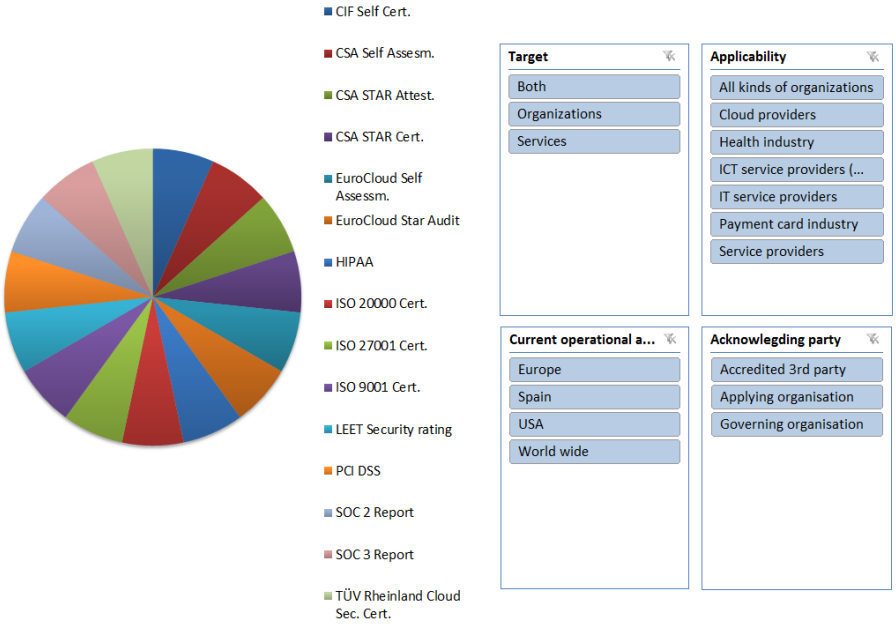

Figure 6.1: Pivot chart before filtering of the assessment schemes

Looking instead at Figure 6.2, a filtering has been performed with a selection according to the opinions from the interviews. Since the cloud platform is only a part of Ferranti's business, it has to be an assessment scheme that is targeting

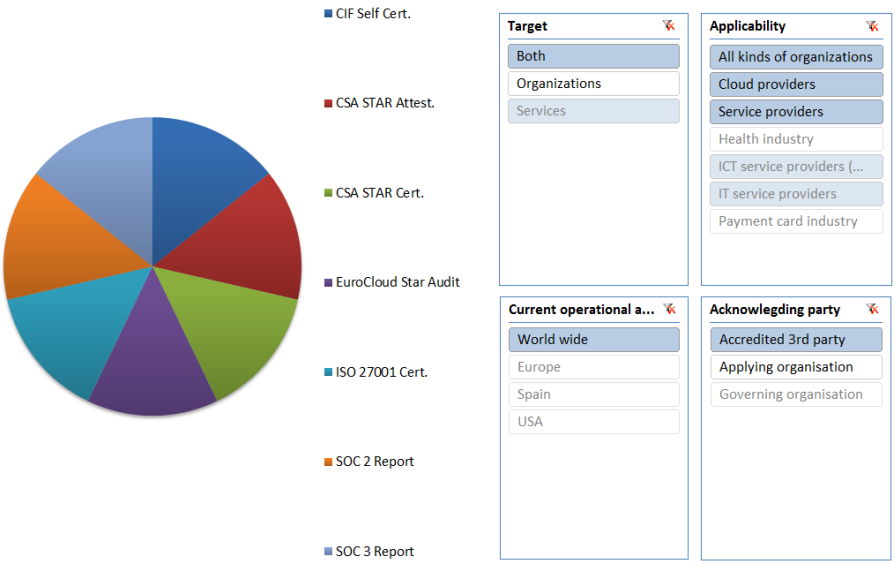

Figure 6.2: Pivot chart after filtering of the assessment schemes

services and not only whole organisations. Therefore, *Organizations* has been deselected in the target-box. Since Ferranti have future plans to expand from their European market to America and Asia, it should be an assessment scheme that is recognized world wide. Therefore, *World wide* has been selected as only option in the box for current operational area. Due to Ferranti's Quality and Business Process Manager's wish of having a quality auditor, *Accredited 3rd party* has been exclusively chosen in the box for acknowledging party. Last but not least, in the applicability box the very specific options *Health Industry* and *Payment card industry* have been deselected. This to make sure it is an assessment scheme, with a not too narrow scope.

	Access by unauthorized users	Several customers on the same platform	Deviating IT-security policy	Inaccessible data
CIF Self Cert.	✓	~	✓	~
CSA STAR Attest.	✓	✓	✓	✓
CSA STAR Cert.	✓	✓	✓	✓
EuroCloud Star Audit	✓	~	✓	✓
ISO 27001 Cert.	✓	~	✓	✓
SOC 2 Report	✓	~	✓	✓
SOC 3 Report	✓	~	✓	✓

✓	Fully addressed
~	Partly addressed

Table 6.1: Known cloud risks addressed by the remaining assessment schemes

By carrying out this filtering, the original list of assessment schemes got reduced drastically. To see how the remaining assessment schemes scored in the risk comparison an extraction from Table 4.2, showing known cloud risks addressed per assessment scheme, was made. This extraction only holds the reduced list of assessment schemes, and can be seen in Table 6.1.

As a last comparison point it was examined how recognized the assessment schemes, in the reduced list, were among Ferranti's employees and customers. This was done by simply counting how many times an assessment scheme was referred to in the RFPs as well as how many of the interviewees that stated that they had heard about an assessment scheme before. The result can be seen in Table 6.2, where it is also highlighted which one that turned out to be, by far, the most recognized one.

Certifications & standards	Referred to in RFP's	Recognized by Ferranti employee's
CIF Self Cert.	-	-
CSA STAR Attest.	-	I
CSA STAR Cert.	-	I
EuroCloud Star Audit	-	-
ISO 27001 Cert.	III	IIII
SOC 2 Report	-	III
SOC 3 Report	-	III

Table 6.2: Recognition of assessment schemes among Ferranti customers and employees

A compilation of the risk comparison and the recognition comparison can be seen in Table 6.3. Based on this compilation, the decision was made of moving further with the three options CSA Star Attestation, CSA STAR Certification as well as ISO 27001 Certification.

Certifications & standards	Risk comparison	Recognition
CIF Self Cert.	×	×
CSA STAR Attest.	✓	~
CSA STAR Cert.	✓	~
EuroCloud Star Audit	~	×
ISO 27001 Cert.	~	✓
SOC 2 Report	~	~
SOC 3 Report	~	~

✓	Good
~	Moderate
×	Bad

Table 6.3: Compilation of the risk comparison and the recognition comparison

6.2 Last Comparison of Chosen Assessment Schemes

The final decision of which assessment scheme to go for, was put in the hands of Ferranti themselves. To facilitate them in making this decision, a SWOT analysis for each one of the three remaining assessment schemes was created.

These can be found in Figure 6.3, 6.4 and 6.5.

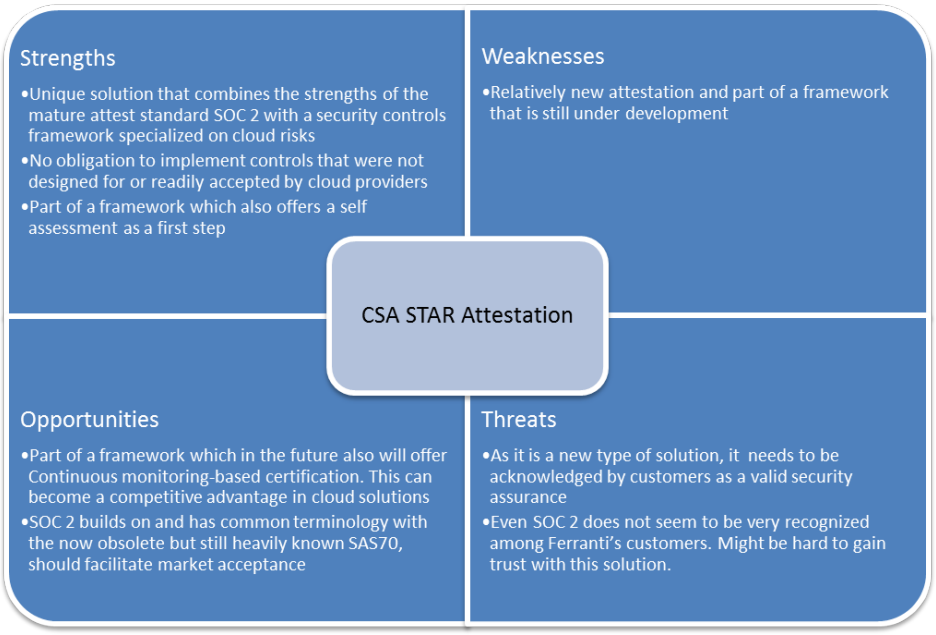

Figure 6.3: SWOT analysis of CSA STAR Attestation

After careful consideration of the SWOT analyses, Ferranti decided that they wanted to go further with the CSA STAR Certification (Figure 6.4). There were several reasons to this decision. First of all they preferred an assessment scheme that includes acquiring the ISO 27001, which is requested by many of their customers. For this reason they opted out the CSA STAR Attestation (Figure 6.3).

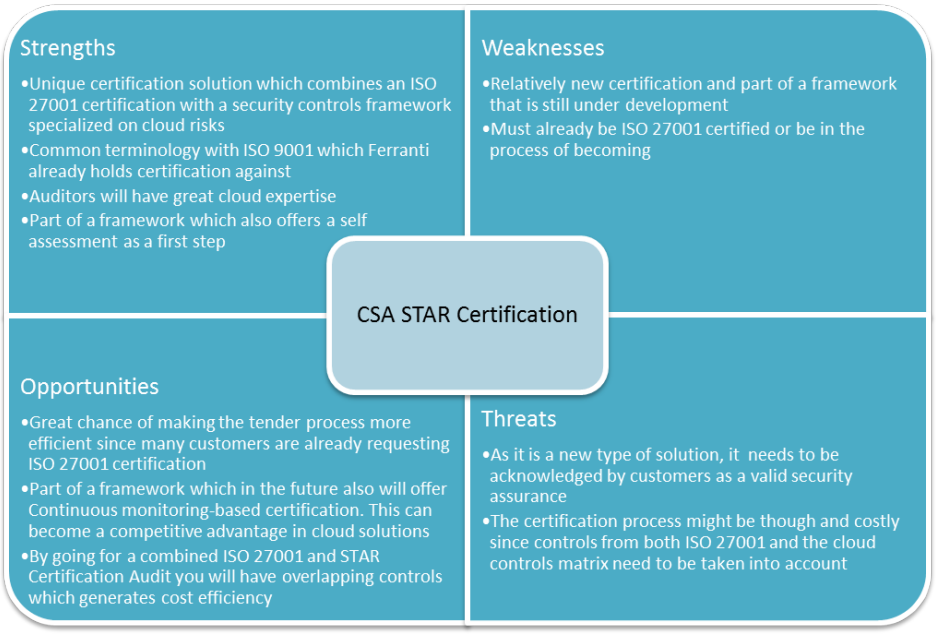

Figure 6.4: SWOT analysis of CSA STAR Certification

Second, they wanted an assessment scheme that is focused on mitigating risks in a cloud environment. As shown in the risk comparison in Chapter 4, the ISO 27001 Certification (Figure 6.5) does not address all risks that are created when data is moved to the cloud. The ISO 27001 certification was created before the new challenges around cloud services arose and assures information security only on a more general level. The same conclusion was drawn in the paper *Analysis of ISO 27001:2013 Controls effectiveness for Cloud Computing* [58], where the following is stated in the abstract: "We come to the conclusion that ISO / IEC 27001:2013 compliance improves service providers and customer's information security system and build a trust relationship but not fulfil all requirements and cover all relevant issues."

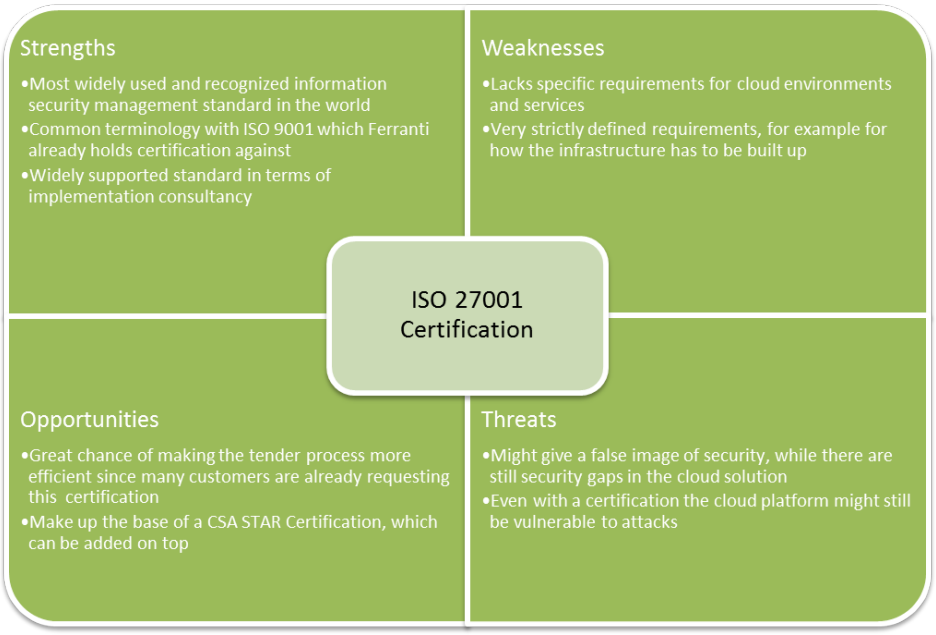

Figure 6.5: SWOT analysis of ISO 27001 Certification

Chapter 7

The certification process

Once the decision for the most suitable assessment scheme was made, the question arose on how to move further towards achieving it. Which steps would need to be carried out to reach the CSA STAR Certification? For that reason, some guidance for the CSA STAR Certification process is in this chapter presented.

7.1 CSA Self Assessment

The final goal for Ferranti is to acquire the CSA STAR Certification. However, CSA strongly recommends all companies to start with completing the CSA Self Assessment. This can be done either by filling in the CSA CAIQ or by creating a personal report documenting compliance to the CSA CCM. The easiest option is probably to fill in the CSA CAIQ. This questionnaire holds a list of control specifications, which has been divided into 16 domains and 295 questions. Each of these questions can be answered with simply "Yes", "No" or "Not applicable". A cutout from the questionnaire can be found in Figure 7.1.

CAIQv3.0.1 CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.0.1

Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers		
					Yes	No	Not Applicable
Application & Interface Security *Application Security*	AIS-01	AIS-01.1	Applications and programming interfaces (APIs) shall be designed, developed, deployed and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	Do you use industry standards (Build Security in Maturity Model [BSIMM] benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST, etc.) to build in security for your Systems/Software Development Lifecycle (SDLC)?			
		AIS-01.2		Do you use an automated source code analysis tool to detect security defects in code prior to production?			
		AIS-01.3		Do you use manual source-code analysis to detect security defects in code prior to production?			
		AIS-01.4		Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?			
		AIS-01.5		(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?			

Figure 7.1: Cutout from the CSA CAIQ, showing the first control specification from the domain Application & Interface Security

The second option for the self assessment is to use the CSA CCM. This tool contains the same list of control specifications, divided into domains, as the CSA CAIQ. However, the domains are not further divided into specific questions. Instead the provider has to create a report documenting compliance to the CSA CCM. On the other hand, the CSA CCM has the advantage that it shows how the controls map to other industry-accepted security standards, regulations, and controls frameworks. A cutout from the matrix can be found in Figure 7.2.

CCMv3.0.1 CLOUD CONTROLS MATRIX VERSION 3.0.1

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ISO/IEC 27001-2013	ITAR	Jericho Forum
Application & Interface Security Application Security	AIS-01	Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	A9.4.2 A9.4.1, 8.1*Partial, A14.2.3, 8.1*partial, A.14.2.7 A12.6.1, A18.2.2		Commandment #1 Commandment #2 Commandment #4 Commandment #5 Commandment #11
Application & Interface Security Customer Access Requirements	AIS-02	Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed.	A9.1.1.		Commandment #6 Commandment #7 Commandment #8
Application & Interface Security Data Integrity	AIS-03	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.	A13.2.1, A13.2.2, A9.1.1, A9.4.1, A10.1.1 A18.1.4		Commandment #1 Commandment #9 Commandment #11

Figure 7.2: Cutout from the CSA CCM, showing the three first control specification from the domain Application & Interface Security and how they map to controls in ISO 27001:2013 and Jericho Forum

In the end, this report or the CSA CAIQ can be submitted to the CSA and they will display it on their website. Even if the CSP does not want to submit the result of the self assessment, it is a great starting point for the certification process. First of all it will help CSPs understand the background to why certain things need to be implemented. Second, it will open their eyes to possible security gaps in their current solutions.

7.2 Gain management support

No matter how close to, or far away from, security perfection your cloud solution is, management support will be essential. A certification process will always be costly and management has to be willing to make the investment. Furthermore, to successfully achieve and keep the certification, all employees have to feel motivated to work according to certain principles and understand why it is important to do so. This can only be achieved if management understands the benefits of certification and propagates it within the organisation.

In one of the interviews that was carried out (Chapter 5), the interviewee explained that to gain management support, you have to convince them that the

investment will have a clear return on investment. This can be done in several different ways but one way of doing it will be to use the CSA CAIQ. By going through the questions with 'No' as answer, management will become aware of the security gaps that exist at the moment. For efficiency diagrams can be created, that display in which domains the biggest gaps are, an example can be found in Figure 7.3.

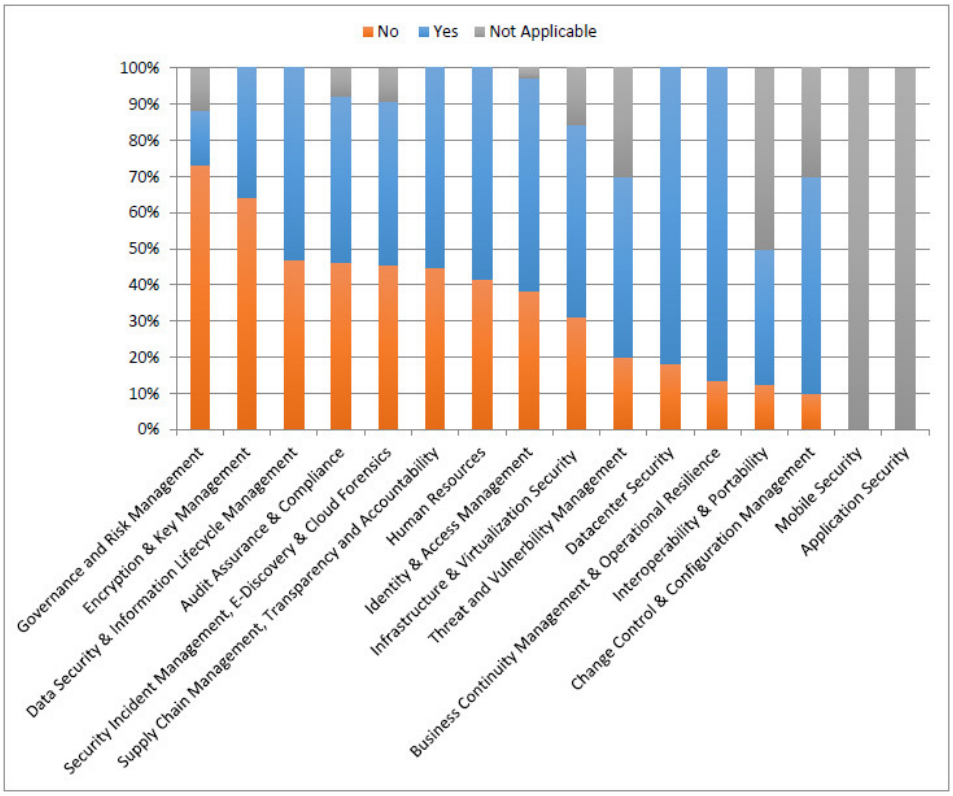

Figure 7.3: Diagram showing answer percentage per domain from the CSA CAIQ. Domains are listed according to the percentage of controls not in place. This makes it is easy to see which domains that currently hold the biggest security gaps.

In relations to the security gaps, it is important to explain the consequences they can bring and what sort of threats the platform is exposed to for the moment. An overlooked risk can cause big damage and usually results in huge price tags for recovery. Some price examples can be found in [59], wherein it is also stated that "Leading research companies Gartner and Forrester both agree that the costs of prevention are much lower than the costs of recovery after an attack or data theft."

To explain to management what needs to be done to minimize the security gaps and how much the solutions will cost, Table 7.1 can be used.

Solution	CID	Investment	Internal resources	External resources
Firewall	AIS-01.1	1	1	2
⋮	AIS-01.5	3	2	3
⋮	BCR-01.1	4	1	1
⋮	CCC-04.1	1	4	1
⋮	DSI-05.1	3	4	4
⋮	GRM-01.3	1	1	4
⋮	GRM-09.2	5	1	5

Weighing scale	Investment (EUR)	Resources (MD)
1	<5000	1 - 5
2	5000-10000	5 - 10
3	10000-25000	10 - 25
4	25000-50000	25 - 50
5	>50000	>50

Table 7.1: Table to be used in assessing finances and resources needed in the certification project

The table works as an addition to the CAIQ. For every question that has been answered with 'No', a proposition of a possible solution must be given. Then an estimation must be made how much this solution will cost in terms of hardware/software as well as how many internal or external resources, in terms of man days, that will be needed to implement the solution. In the end a diagram can be made displaying which questions or controls that are cheapest to implement and which require least resources. An example of such a diagram can be seen in Figure 7.4. Weighting factors have been used in Table 7.1 to give the diagram a nice shape.

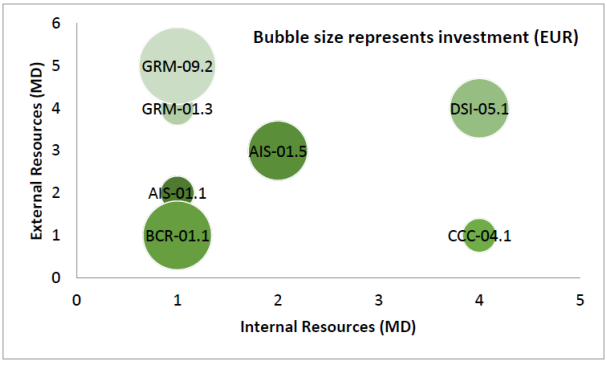

Figure 7.4: Diagram to visualize which solutions that will be cheapest or least resource consuming to implement

In addition to this some sort of priority order will need to be made, showing which controls that represent the biggest security risks and therefore are most valuable and urgent to implement.

7.3 From project plan to finalization

Once management support has been gained, the next step for the project team will be to take a closer look at what needs to be achieved to reach the certification. Table 7.1 and Figure 7.4 can be used as a base for this, since they show a preliminary assumption of the work ahead. To reach more realistic numbers the project team needs to logically regroup the different solutions into clearly defined separate projects. Attaining of a certification is a huge task and requires detailed planning in terms of time and resources. With a clearer view on the seperate projects, the project team can make a better estimation of cost and man days of resources. Table 7.1 and Figure 7.4 can be used as aids in making the new estimates. The end result will be a feasibility study which can be presented to top management. In this meeting it is important to point out the quick wins of each milestone in the roadmap. With a good general assessment of the project costs and benefits, management will hopefully give their final approval.

The real project work can now start by creation of project outlines for the first group of projects. A project outline is an A4 page in which one shortly introduces the project. It should include the goals and expectations, specify the people involved (internal and external), present the budget needed and show the big steps of the project in a timeline. Based on the project outlines the (by management appointed) project sponsor can make a decision to make the different resources (people and investments) available to the team.

The general planning and decision phase is then finished and one can start with the execution of the projects. A good project manager needs to continuously inform the sponsor about the progress of the project. This is usually done through project reports. After finishing each project the project manager needs to write a project review to seek continuous improvement in the team's work.

When the project is finally finished the team needs to write a support and maintenance plan. The finished project can then be transferred to the operational team.

Section 7.2 and 7.3 are based on the course Software Engineering Process - Economy and Quality at Lund University and its belonging course literature [60].

Chapter 8
Discussion and Conclusions

This thesis has investigated the matter of assessment schemes for CSPs. In particular assessment schemes that helps CSPs prove to their customers that their services are secure. Many different assessment schemes, for this purpose, can be found on the market today but not many good ways of comparing them. This problem was identified and to solve it the following three goals were defined for this thesis:

- Create a clear overview of the cloud assessment schemes that exists on the market
- Provide methods to categorize or compare assessment schemes
- Make a case study on Ferranti demonstrating how the accomplishments can be put to practice

To live up to those goals, three main deliveries were created. First of all an overview including a short explanation of relevant assessment schemes on the market. Second, a comparison of assessment schemes in terms of risk mitigation. Third, a case study on Ferranti where previous findings in combination with results from interviews were used to select a suitable assessment scheme for Ferranti's cloud platform.

8.1 Discussion

Looking at the first of the three goals, it was fulfilled through the cloud assessment schemes overview in Chapter 3. However, something that needs to be mentioned in relation to this, is the difficulty encountered in defining which assessment schemes to include in the overview. Originally all sort of assessment schemes that could be relevant for CSPs were supposed to be included. However, after a while it was recognized that this would be an impossible task. There are an uncountable number of assessment schemes out there and the relevance of those will be dependent on the CSP. Things that matter are for example what sort of data they want to store on the platform, or in which country their customers are operating. Furthermore, the relevance will also be dependent on the reason to certification or similar target. Some CSPs might look into assessment schemes to assure security, while others are looking into it to assure quality.

As mentioned earlier, the creation of the overview began with a very wide scope. Since it was recognized only along the way that the scope needed to be narrowed down, the end result became a bit scattered. The majority of the assessment schemes included, are focused on assuring security in a cloud environment. However, there are also assessment schemes with completely different focuses and scopes.

Something else that hampered the creation of the overview, was the amount of questionable or incorrect sources of information. Several sources claimed quite the opposite to each other. A lot of misunderstandings had been made along the way and to clear those out took a substantial amount of time.

The next goal was to provide methods to categorize or compare assessment schemes. In Table 5.1 a sort of categorization of most of the assessment schemes in the overview was made. After creation of the overview, it was concluded that some of the assessment schemes within it were less relevant for CSPs. Therefore, these were not included in Table 5.1 or the rest of the investigation.

In addition to Table 5.1, a risk comparison in terms of risk mitigation was carried out. The decision was made to concentrate on assessment schemes with a focus on assuring security in a cloud environment. Therefore, it was considered interesting to see how well they addressed known cloud risks. As described in Chapter 4, the comparison was based on ENISA's CCSM and its security objectives. To map the defined cloud risks to these security objectives, turned out to be quite challenging since there is not really a right and wrong. The descriptions of the security objectives were very general and sometimes a bit unclear. They had to be gone through carefully, several times, before a satisfactory result was reached. With these things being mentioned the second goal is considered fulfilled.

The third goal was to make a case study on Ferranti demonstrating how the accomplishments can be put to practice. Looking through the chapters above, it is easy to see how the filtering and the SWOT analysis in Chapter 6 are based on all the previous discoveries. The SWOT analyses led Ferranti to the final decision of moving on further with CSA STAR Certification. Almost no one at Ferranti had heard about this certification before and most of them were convinced that the ISO 27001 certification would be the best alternative. The research opened their eyes to other options and made them change their mind. This serves as a clear proof that the findings were put to good use and that the third goal is hereby accomplished.

8.2 Conclusions

In the creation of the cloud assessment overview, it turned out to be really difficult to find trustworthy sources. As mentioned above, many sources were not clearly defined and some even proved contradictory. Seeing this it could be concluded that there is a great uncertainty surrounding these sort of assessment schemes. Therefore an investigation like this was more than necessary and it can hopefully be of great value to many companies.

When carrying out the case study on Ferranti it became obvious that the most known assessment scheme is not always the best one. As can be seen in Table 6.2

the ISO 27001 certification was, by far, the most recognized one. However, the risk comparison in Chapter 4 and in particular Table 4.2, shows that the ISO 27001 certification leaves some things to be desired in terms of risk mitigation in the cloud.

In the introduction, there was a general question regarding if it really has to be as hard as unveiling a great mystery, to understand the world of assessment schemes. Speculations were made concerning if it was possible to assemble and present relevant assessment schemes in plain English and if there was a way to compare or categorize them? By glancing through this report, anyone can conclude that there are ways to make the world of assessment schemes more transparent. This thesis is unique in the way that it both proves the need of clarity and shows methods to achieve it.

8.3 Future work

The work carried out in this project represent one way of making the world of assessment schemes less complex. Other methods can most likely be found and the work in this thesis can definitely be expanded.

New assessment schemes or updates of existing ones are published on a regular basis. As a consequence, the work with presenting and comparing them can continue in eternity. As the cloud and its associated services matures, the way of proving that they are secure will most likely also mature. This should make the future work of surveying assessment schemes easier.

The main goals of this thesis were all reached. However, another point discussed in the introduction, was that it is hard to see exactly how the different assessment schemes are overlapping. It would be of great value to investigate which controls in the different assessment schemes that are similar to each other. In this way, a company holding one to begin withr official security recognition, could easily see how many and which controls they need to implement to reach others.

References

All URLs were last accessed on 5 January 2016.

[1] KPMG Support Services, *The Retirement of SAS 70*, www.kpmg.com/be/en/issuesandinsights/articlespublications/the-kpmg-difference/pages/the-retirement-of-sas-70.aspx

[2] The Official SSAE 16 Resource Guide, *SSAE 16 and ISAE 3402 |Two Common Standards*, www.ssae16.org/what-is-ssae-16/ssae-16-and-isae-3402.html

[3] Deloitte Luxembourg, *ISAE 3402 ans SSAE 16 (replacing SAS 70) Reinforcing confidence through demonstration of effective controls*, www2.deloitte.com/content/dam/Deloitte/lu/Documents/risk/lu_en_isae3402-ssae16_04072014.pdf

[4] Dave Shackleford, *Using SSAE 16 standard, SOC reports to assess cloud provider security*, searchcloudsecurity.techtarget.com/tip/Using-SSAE-16-standard-SOC-reports-to-assess-cloud-provider-security

[5] Stichting Corporate Governance, *How is ISAE 3000 related to ISAE 3402*, www.isae3000.com/isae-3000-and-isae-3402

[6] The SSAE 16 Guide, *What is AT-101?*, www.ssae16guide.com/ssae-16/what-is-at-101

[7] Mayank Trivedi, *Misconceptions around SSAE 16 / ISAE3402*, www.isaca.org/Blogs/138859/Lists/Posts/ViewPost.aspx?ID=2

[8] Debbie Zaller, *Is there a SOC certification similar to an ISO 27001 certification?*, www.brightline.com/2015/06/soc-2-similar-to-iso-27001

[9] Margaret Rouse, *ISO 9000 definition*, searchdatacenter.techtarget.com/definition/ISO-9000

[10] Perry Johnson Registrars, *Benefits of ISO 9000*, www.pjr.com/standards/iso-90012008/benefits-of-iso-9000

[11] International Organization for Standardization, *ISO 9000 - Quality management*, www.iso.org/iso/iso_9000

[12] Jean-François Pillou, *ISO 9000, ISO 9001 and ISO 9004*, http://ccm.net/contents/614-iso-9000-iso-9001-and-iso-9004

[13] The 9000 Store, *What is ISO 9004:2009 for continual improvement*, http://the9000store.com/what-is-iso-9004.aspx

[14] David Wealleans (2005), *The Quality Audit for ISO 9001:2000*, ISBN-13: 978-056-608-598-7, page 58.

[15] 27001Academy, *ISO 27001 vs. ISO 27002*, http://advisera.com/27001academy/knowledgebase/iso-27001-vs-iso-27002/

[16] ZBC kennisbank, *Nu ook certificatieschema voor iso 27002 beschikbaar*, http://zbc.nu/security/iso-27002-maatregelen-informatiebeveiliging/nu-ook-certificatieschema-voor-iso-27002-beschikbaar/

[17] IsecT Ltd, *FAQ: "How does my organization get certified against ISO/IEC 27002?"*, www.iso27001security.com/html/audit_-_certification.html#CertifyTo27002

[18] International Organization for Standardization, *ISO/IEC 27001:2013*, www.iso.org/iso/catalogue_detail?csnumber=54534

[19] International Organization for Standardization, *ISO/IEC 27002:2013*, www.iso.org/iso/catalogue_detail?csnumber=54533

[20] Edward Humphreys, *ISO/IEC 27000: get to know the family*, www.irca.org/en-gb/resources/INform/archive/issue25/Features/ISO-IEC-27000

[21] Certification & Information Security GmbH, *ISO 27K: Supplementary standards as implementation and operation aid*, www.cis-cert.com/System-Certification/Information-Security/ISO-27001/ISO-27k.aspx

[22] Davey Winder, *How can ISO 27017 and 27018 help secure the cloud?*, www.cloudpro.co.uk/cloud-essentials/cloud-security/5004/how-can-iso-27017-and-27018-help-secure-the-cloud

[23] Lynda Cooper, *ISO/IEC 20000 – An Evolving Series*, blog.apmg-international.com/index.php/2015/01/29/isoiec-20000-an-evolving-series

[24] IT Governance Ltd, *ISO20000-4 (ISO 20000-4) Process Reference Model*, www.itgovernance.co.uk/shop/p-686-iso20000-4-iso-20000-4-process-reference-model.aspx

[25] International Organization for Standardization, *ISO/IEC TR 20000-5:2013*, www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=60329

[26] Lynda Cooper, *ISO/IEC 20000 Part 9 – Guidance on the Application of ISO/IEC 20000-1 to Cloud Services*, blog.apmg-international.com/index.php/2015/03/19/isoiec-20000-part-9-guidance-on-the-application-of-isoiec-20000-1-to-cloud-services

[27] 20000Academy, *ISO 20000 and ITIL – How are they related?*, http://advisera.com/20000academy/knowledgebase/iso-20000-and-itil-how-are-they-related/

[28] Drago Topalovic (2014), *ITIL vs. ISO/IEC 20000: Similarities and Differences & Process Mapping*

[29] Vivienne Rojas, *The importance of framing the cloud*, www.iso.org/iso/home/news_index/news_archive/news.htm?refid=Ref1897

[30] Cloud Security Alliance, *Open Certification Framework, Vision Statement, Rev. 1*, downloads.cloudsecurityalliance.org/initiatives/ocf/OCF_Vision_Statement_Final.pdf

[31] Cloud Security Alliance, *CSA STAR: The Future of Cloud Trust and Assurance*, https://cloudsecurityalliance.org/star/#_overview

[32] Cloud Security Alliance, *Introduction to the Cloud Controls Matrix Working Group*, https://cloudsecurityalliance.org/group/cloud-controls-matrix

[33] Cloud Security Alliance, *Introduction to the Consensus Assessments Working Group*, https://cloudsecurityalliance.org/group/consensus-assessments

[34] Cloud Security Alliance, *STAR Certification & STAR Attestation Submission*, https://cloudsecurityalliance.org/star/#_submit

[35] BrightLine CPAs & Associates, Inc., *Understanding the Cloud Security Alliance STAR Program – Certification and Attestation*, www.brightline.com/2015/02/understanding-star

[36] Cloud Security Alliance, *About CSA STAR Continuous*, https://cloudsecurityalliance.org/star/continuous

[37] CloudWATCH, *Cloud certification guidelines and recommendations*, cordis.europa.eu/docs/projects/cnect/4/610994/080/deliverables/001-D41Cloudcertificationguidelinesandrecommendationsrevisedversion.pdf

[38] EuroCloud Europe, *Why the ECSA?*, https://eurocloud-staraudit.eu/home/value.html

[39] EuroCloud Europe, *ECSA Self Assessment*, https://eurocloud-staraudit.eu/certificates/ecsa-self-assessment-report.html

[40] PCI Security Standards Council, *PCI DSS Quick Reference Guide - Understanding the Payment Card Industry Data Security Standard version 3.1*, www.pcisecuritystandards.org/documents/PCIDSS_QRGv3_1.pdf

[41] TÜV Rheinland, *Cloud Security Certification*, www.tuv.com/en/corporate/business_customers/information_security_cw/strategic_information_security/cloud_security_certification/cloud_security_certification.html

[42] Fabasoft Cloud GmbH, *The Fabasoft Cloud awarded "Certified Cloud Service" status by TÜV Rheinland*, www.fabasoft.com/cloud/en-uk/fabasoft-cloud-awarded-certified-cloud-service-status-tuev-rheinland

[43] LEET Security, *Noticias*, www.leetsecurity.com/noticias

[44] LEET Security, *The agency*, www.leetsecurity.com/la-agencia

[45] LEET Security (2015), *Rating detailed guide*, pages 3-4, 9.

[46] Cloud Industry Forum, *The Cloud Industry Forum Cloud Service Provider Code of Practice: An Executive Briefing*, http://cif-dev.sites.ac/sites/default/files/CIF%20CoP%20Document%201_An%20Executive%20Briefing_%281.0%29.pdf

[47] Cloud Industry Forum, *Code of Practice for Cloud Service Providers*, http://cloudindustryforum.org/code-of-practice/cop

[48] Cloud Industry Forum, *Self-Certification Process*, www.cloudindustryforum.org/content/self-certification-process

[49] Cloud Industry Forum, *COP Detailed Overview*, www.cloudindustryforum.org/content/cop-detailed-overview

[50] Margaret Rouse, *HIPAA (Health Insurance Portability and Accountability Act) definition*, searchdatamanagement.techtarget.com/definition/HIPAA

[51] ENISA, *Health Insurance Portability and Accountability Act*, www.enisa.europa.eu/activities/risk-management/current-risk/laws-regulation/data-protection-privacy/health-insurance-portability-and-accountability-act

[52] Morgan Brown, *Should app developers get HIPAA certified?*, www.truevault.com/blog/should-app-developers-get-hipaa-certified.html

[53] TrueVault, *HIPAA compliance*, www.truevault.com/hipaa-compliance.html

[54] Margaret Rouse, *HITECH Act (Health Information Technology for Economic and Clinical Health Act) definition*, searchhealthit.techtarget.com/definition/HITECH-Act

[55] U.S. Department of Health & Human Services, *HITECH Act Enforcement Interim Final Rule*, www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html

[56] Roger A. Grimes, *The 5 cloud risks you have to stop ignoring*, www.infoworld.com/article/2614369/security/the-5-cloud-risks-you-have-to-stop-ignoring.html?page=2

[57] ENISA, *Cloud Certification Schemes Metaframework*, resilience.enisa.europa.eu/cloud-computing-certification/list-of-cloud-certification-schemes/cloud-certification-schemes-metaframework

[58] Muhammad Imran Tariq and Vito Santarcangelo. *Analysis of ISO 27001:2013 Controls Effectiveness for Cloud Computing.* In Proceedings of the 2nd International Conference on Information Systems Security and Privacy - ICISSP 2016, ed. by Olivier Camp, Steven Furnell and Paolo Mori, SCITEPRESS – Science and Technology Publications, Lda., ISBN 978-989-758-167-0, pages 201-208. ICISSP 2016, February 19-21, 2016.

[59] László Dellei, Balabit (2015), *ISO 27001 - Let's make the impossible possible!*, pages 4-5.

[60] Bob Hughes and Mike Cotterell, McGraw Hill (2009), *Software Project Management 5:th ed*, ISBN-13: 978-007-712-279-9, pages 22-23, 35-36, 51, 103-106, 323-334.

LUND
UNIVERSITY

Series of Master's theses
Department of Electrical and Information Technology
LU/LTH-EIT 2016-483

http://www.eit.lth.se