TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies
TTU IT College

Mark-Kristjan Markson 179939IVSB

SECURE CLOUD SERVICE - COMPARISON OF ISKE B 1.17 AND BSI C5 BASED ON A CLOUD SERVICE PROVIDER

Bachelor's thesis

Supervisor: Valdo Praust
MSc

Tallinn 2020

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond
TTÜ IT Kolledž

Mark-Kristjan Markson 179939IVSB

TURVALINE PILVETEENUS - ISKE B 1.17 JA BSI C5 VÕRDLEMINE ETTEVÕTTE PILVETEENUSE NÄITEL

bakalaureusetöö

Juhendaja: Valdo Praust
Magistrikraad

Tallinn 2020

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Mark-Kristjan Markson

31.03.2020

Abstract

The aim of present thesis is to compare differences between two cloud security frameworks and as a practical work, compare Cloud Service Providers (CPS) standards with authors chosen cloud security framework to verify if CSP's current standards are up to par with the frameworks standards. The work will give an overview of two cloud security frameworks, theoretical comparison analysis of the two frameworks and result of real-life comparison of a framework and an enterprise cloud service.

During the thesis both theoretical and practical analysis will be conducted. Theoretical analysis will give a comparison overview of the two frameworks. Practical work will compare frameworks standards with the CSP existing standards.

The result of this thesis is to determine if CSP meets all the standards of the framework and if needed give suggestions on how to improve them where needed.

This thesis is written in English and is 36 pages long, including 5 chapters, 7 figures.

Annotatsioon

Käesoleva töö eesmärgiks on võrrelda erinevusi kahe pilveteenuse turvaraamistiku vahel ning praktiliselt võrrelda raamistike standardeid pilveteenuse pakkuja standarditega. Töö annab ülevaate kahest turvaraamistikust, teoreetilise võrdleva analüüsi ning reaalse ettevõtte pilve-teenuse võrdluse raamistiku põhjal.

Töö käigus viiakse läbi teoreetiline ja praktiline osa ning analüüs. Teoreetiline analüüs annab võrdleva ülevaate kahest pilve turvaraamistiku moodulist. Praktilises osas tehakse võrdlus ettevõtte ja raamistiku standartide vahel ning puuduste korral antakse soovitusi, kuidas standardeid parandada.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 36 leheküljel, 5 peatükki, 7 joonist.

List of abbreviations and terms

CSP	Cloud Service Provider

Table of Contents

List of figures 9
Introduction 10
1 Description of the problem and formulation of the assignment 12
1.1 General Overview 12
1.2 Limitations 13
1.3 Description of the problem and the goal of this work 13
2 Methodology 14
2.1 Theoretical part 14
2.2 Practical part 14
2.2.1 Practical solution 14
2.2.2 Practical solution analysis 15
3 Comparison and analysis of BSI C5 and ISKE B 1.17 modules 16
3.1 Introduction to cloud security frameworks 16
3.1.1 ISKE B 1.17 16
3.1.2 BSI C5:2020 17
3.2 Overall structure and control dependencies 18
3.3 Similarities between BSI C5 and ISKE B 1.17 20
3.3.1 Security Policies 20
3.3.2 Cryptography 20
3.3.3 Audit 21
3.3.4 Cloud Service Provider Contracts 21
3.4 Differences between BSI C5 and ISKE B 1.17 21
3.5 The Value of ISKE B 1.17 22
4 Practical result analysis 23
4.1 Organisation of Information Security (OIS) 23
4.2 Security Policies and Instructions (SP) 23
4.3 Personnel (HR) 24
4.4 Asset Management (AM) 24
4.5 Physical Security (PS) 25
4.6 Operations (OPS) 25

4.7 Identity and Access management (IDM) 26
4.8 Cryptography and Key Management (CRY) 26
4.9 Communication Security (COS) 27
4.10 Portability and Interoperability (PI) 27
4.11 Procurement, Development and Modification of Information Systems (DEV) 27
4.12 Control and Monitoring of Service Providers and Suppliers (SSO) 28
4.13 Security Incident Management (SIM) 28
4.14 Business Continuity Management (BCM) 29
4.15 Compliance (COM) 29
4.16 Dealing with investigation requests from government agencies (INQ) 29
4.17 Product Safety and Security (PSS) 30
4.18 Conclusion of practical solution 30
5 Summary 33
References 34
Appendix 1 – Practical work 36

List of figures

Figure 1 Control comparison diagram of C5 and B 1.17 (Source: Author created)..... 13
Figure 2 Structure of the thesis (Source: Author created)..... 14
Figure 3 Structure of C5 Criteria Catalogue (Source: Author created)..... 17
Figure 4 Structure of the Criteria (Source: Author created)..... 18
Figure 5 C5 criteria dependency schema between Areas (Source: Author created) 19
Figure 6 B 1.17 module dependency schema (Source: Author created) 20
Figure 7 Statistics of the met and unmet criteria. (Source: Author created) 31

Introduction

This work deals with analysis of two different cloud security framework modules for securing cloud computing services and infrastructure. These frameworks have a purpose of ensuring safety of client data held within the domain of the Cloud Service Providers (From now on referred by the author as CSP). The work will give an overview of these two frameworks while comparing them and real-life analysis/audit based on an existing cloud service that author has set up for a company.

Security frameworks are usually developed out of need to secure something specific or an overall guideline for computer systems, infrastructure or even human resources. But the cloud computing area is quite specific field.

In this work one of the security frameworks is based on the other one, so this also includes the cloud computing modules of these frameworks. This proposes a question or a problem that does the newer cloud security framework bring any new value to the already existing cloud security frameworks or the cloud security domain. In addition there currently is no academic research comparing the two cloud security frameworks.

The topicality of this work is related to the authors work of setting up the cloud service that will be used in live environment and to replace old cloud system. Use a framework as a checklist to ensure that authors cloud service has security policies and provides adequate protection for cloud customer data. This affects not only the author, but the company as a whole.

The result of this work will be comprehensive review and analysis of these frameworks. Author will point out added value of the newer ISKE cloud security module that is based on BSI and suggest their impact on the cloud security.

The practical solution of this work will be an excel spreadsheet that will provide a checklist based on BSI C5 Criteria Catalogue. All the areas of C5 will be used as a checklist to verify the existing controls of the authors work cloud computing environment. The checklist will provide us with comprehensive result what the company as a CSP

complies with and which criteria it fails to meet. Author will do analysis of the practical work, give a detailed purpose of each area, conclusion of what criteria was met and unmet and also give suggestions on how to improve the CSP security standards based on each area of the C5.

The main research questions that we will try to answer in this work are:

1) Does ISKE B 1.17 that is based on BSI C5 bring any new value to the cloud security and information assurance world and if, what?

2) While comparing these two frameworks – Can we say that while we implement one of these frameworks, the other could also be easily implemented?

3) Is the cloud service that author has set up for the company secure and up to par with frameworks standards?

The topic of this thesis is related to the authors work in real-life by setting up live cloud service for the company and the cloud customers. Author manages all the infrastructure and has used platform called Nextcloud for the cloud service. Such cloud service model is called SaaS or Software as Service.

1 Description of the problem and formulation of the assignment

1.1 General Overview

Over the past decade, IT-industry and the governments have put much more emphasis on the cloud computing. Ever greater efforts have been put into countering cyber-threats and vulnerabilities or loopholes in the cloud domain. Some of the most serious threats for cloud security are:

- Human error
- Denial of Service (DoS/DDoS attack)
- Insecure APIs
- Bad access management
- Data breaches
- Technology vulnerabilities

With an estimated 70% of all organizations using the cloud, cloud security threats should be a concern for every business. [1] The cost of a data breach could be much more that any organization or CSP can afford.

With consistently increasing budgets the exploration of cloud computing security has led to more effective techniques against new vulnerabilities and the creation of more effective security measures or guidelines and standardization of cloud security policies.

These security policies provide us with controls or checklists which enables CSP's to more efficiently implement, improve and maintain information security. This also includes architecture that gives written and visual guidance how to secure, develop and deploy these operations.

In Estonia, the need for such systematic security approach has led to the creation Three-level IT Baseline Security System ISKE which RIA (Republic of Estonian Information System Authority) is said to be meant for the Estonian public sector. [2] ISKE is also said to be mandatory for local governmental institutions that store information assets storage. But the development of ISKE is based on German security framework called BSI-Standard. Hence the need to evaluate the value that the ISKE framework brings to the cloud framework community.

1.2 Limitations

For the practical part of this work author will use one of the frameworks mentioned in this work as a checklist to check the standards of the current cloud environment that author has deployed for his company. This checklist will be added to the appendix of this work and analysed in the practical analysis section of this work.

The implementation of the standards that might be missing will be outside of this works scope, since it may need a bigger planning and more workload than intended for bachelor's thesis and the point of this work.

1.3 Description of the problem and the goal of this work

Since development of the ISKE B 1.17 cloud security module is based on the BSI C5 module. [2] This can arouse a question whether the ISKE cloud module brings any new value to the other popular cloud security frameworks and the cloud security domain itself.

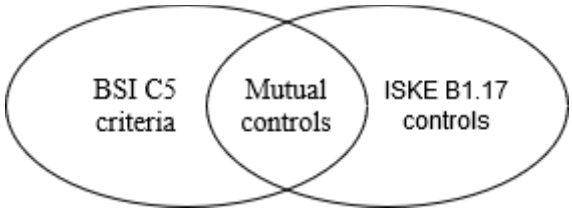

Figure 1 Control comparison diagram of C5 and B 1.17 (Source: Author created)

Using the Figure 1 author should find the mutual controls of the both frameworks. After that preferably we should be able to find additional controls that ISKE B 1.17 offers and analyse them to get the value added by the framework.

2 Methodology

This work will be divided into 2 parts as described in Figure 2:

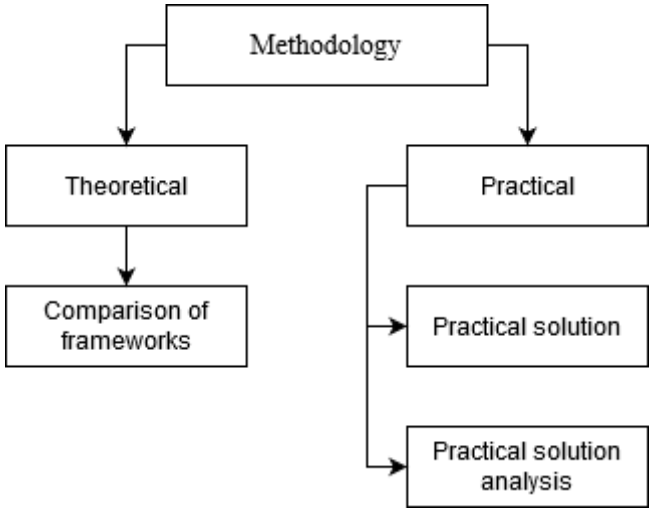

Figure 2 Structure of the thesis (Source: Author created)

2.1 Theoretical part

Theoretical part of this work will use two-step analysis. In first step author will match the controls of BSI C5 with ISKE B 1.17 controls to get the mutual set of controls and then analyse how they are described in each framework.

For the second step author can analyse ISKE controls that are missing from BSI framework and also collect the controls added to the ISKE framework.

2.2 Practical part

2.2.1 Practical solution

For the practical part author has set up a cloud platform called Nextcloud for the CSP which will be compared with a framework including the cloud infrastructure, human resources and security policies. For the most part author wants to put more emphasis on cloud environment such as infrastructure, human resources, assets and policies rather than the application part.

For the practical solution of this thesis author will use the C5 Criteria Catalogue as a checklist to see whether CSP complies with the standards defined in the C5 Catalogue. Author will use C5 because the Nextcloud complies with its and the ISO 27001 standards. [3]

Data for practical solutions will be gathered through interview and documents reviews. Based on the C5 areas author will question whether the company has required documents and will review them based on the requirements of C5.

The result of the practical work will be an excel spreadsheet showing all the areas and controls of the C5 Catalogue, result whether control is already implemented or not and authors reason how the criteria is fulfilled or why the CSP failed to meet the criteria.

2.2.2 Practical solution analysis

The practical solution analysis will describe the result of practical work and C5 in more detail. Analysis will describe goals of each area in the C5 Catalogue. Authors conclusion in each area based on the results of the CSP.

For the final part author will give suggestions on how the CSP could improve in each area where the criteria were no met with C5 standards. After the suggestions for improvements author will display how many criteria were met in the area.

3 Comparison and analysis of BSI C5 and ISKE B 1.17 modules

3.1 Introduction to cloud security frameworks

Overall goal of the cloud security is the protection of data, applications and infrastructure involved in cloud computing. [4] From this goal, a set of rules or functions to achieve the security are created. These rules make up the sophisticated security frameworks.

Cloud security frameworks are like regular security frameworks that provide a list of key functions to manage security related risks in our IT environments, the only difference is that cloud security frameworks are more specific and are mostly related to cloud environment.

Cloud security frameworks can even be modules of regular IT security frameworks and can be implemented separately or mix with other frameworks if the frameworks allow.

In this work author has chosen cloud security modules from two IT-security frameworks called BSI C5 and ISKE B 1.17.

3.1.1 ISKE B 1.17

ISKE B 1.17 is a module of ISKE security framework or Three-level IT Baseline Security System ISKE. Before understanding B 1.17 module one has to understand ISKE itself. Republic of Estonia Information System Authority (RIA) dictates ISKE security framework as the following: “The goal of implementing ISKE is to ensure a security level sufficient for the data processed in IT systems. The necessary security level is achieved by implementing the standard organisational, infrastructural/physical and technical security measures.” [2]

ISKE is based on German information security standard called IT Baseline Protection manual, IT-Grundschutz for short which has been adapted for Estonian needs. [2] The B 1.17 cloud module was added in ISKE version 8.00. The current version that author is working on is the latest version 8.06 of the framework.

3.1.2 BSI C5:2020

BSI C5 is cloud security criteria catalogue of BSI security framework. The BSI framework contain recommendations by the Federal Office for Information Security (BSI) on methods, processes, procedures, approaches and measures relating to information security. [5]

The Cloud Computing Compliance Control Catalogue (C5) was released in BSI:2016 update. In the BSI C5:2016 cloud-specific functions and rules were called privacy controls, in the BSI C5:2020 these controls were renamed to criteria. [6]

In this work author will be working with BSI C5:2020 the latest version that contains 17 main objectives to achieve the security purpose of this framework. Each main objective is future broken down to sub-objectives or criteria required to achieve the main objective as described in Figure 2.

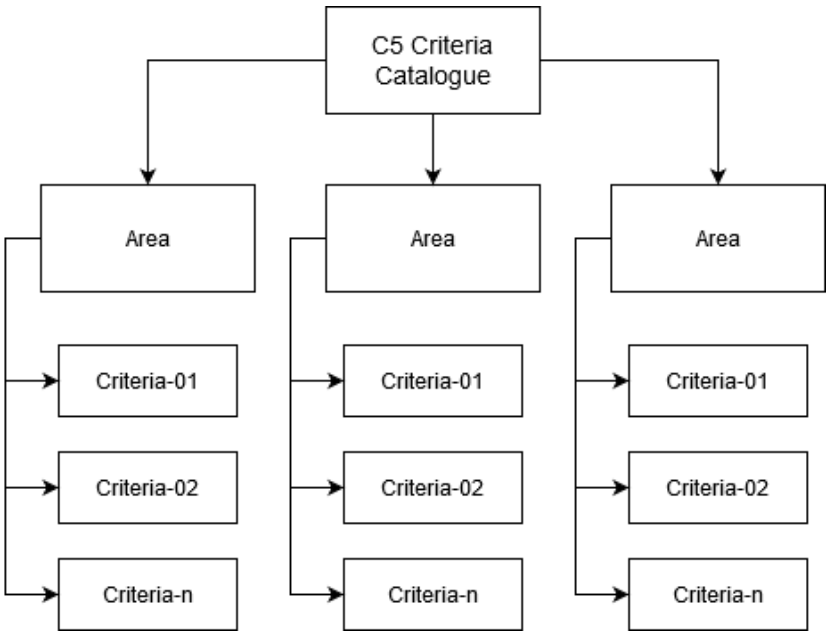

Figure 3 Structure of C5 Criteria Catalogue (Source: Author created)

The C5 criteria are mainly divided into basic, additional criteria and supplementary information. In addition there is complementary customer criterion and information on the possibilities of continuous auditing as described in Figure 3. From BSI standpoint basic criteria means minimum level of information security that that company cloud

service must ensure their customers. Additional criteria may come in handy with customers that have higher protection needs such as government institutions or high-profile clients. Supplementary information gives a bigger picture or overview of the applicable criteria. Complementary customer criterion provides information about what customers could implement with the controls. As the name says continuous auditing provides information about the possibility to continuously monitor the practical aspects of the criterion such as monitor log fails regular scans and more.

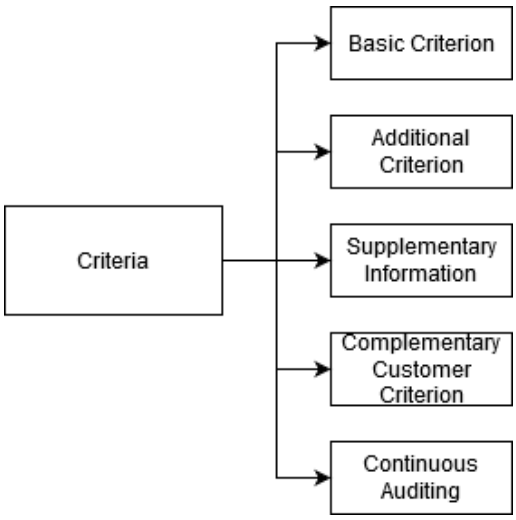

Figure 4 Structure of the Criteria (Source: Author created)

3.2 Overall structure and control dependencies

The structure of BSI C5 is quite straightforward, it pretty much acts as a standalone framework. Only in Organisation of Information Security (OIS) it references the use of ISMS from ISO 27001 standards. C5 does not reference other BSI modules. Some areas like Security Policies and Instructions (SP) act as a dependency for other areas to use as defined policies and instructions as shown on Figure 5.

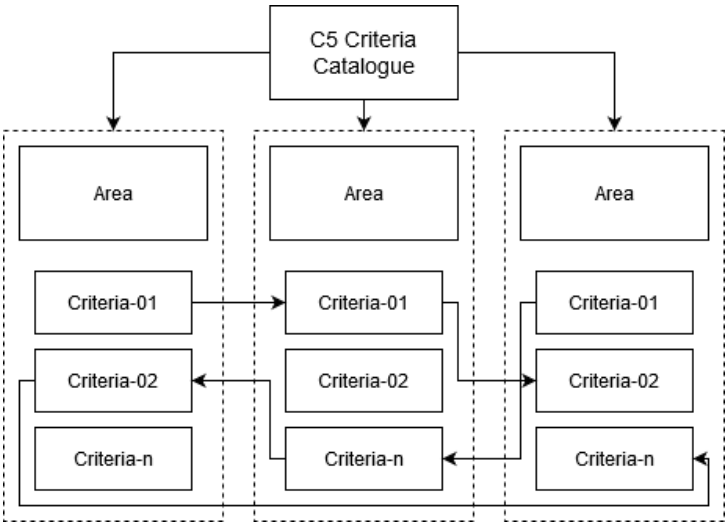

Figure 5 C5 criteria dependency schema between Areas (Source: Author created)

On the other hand the ISKE B 1.17 cloud security module does not act as a standalone cloud security module. It depends on other ISKE framework modules such as:

- Module B 5.21 – Web applications
- Module B 5.24 – Web services
- Module B 3.303 – Storage systems and storage networks
- Module B 3.304 – Virtualization
- Module B 1.7 – Crypto concepts
- Module B 1.11 – Outsourcing
- Module B 1.14 – Security policies management

With this kind of concept, other modules will also have to be addressed, since the B 1.17 is dependent on them and they relate to the cloud environment. On the Figure 6 author shows the B 1.17 dependency structure visualised way. This schema relates only to B 1.17 and does not exclude the possibility of other modules that B 1.17 is depending on, to also depend on other modules.

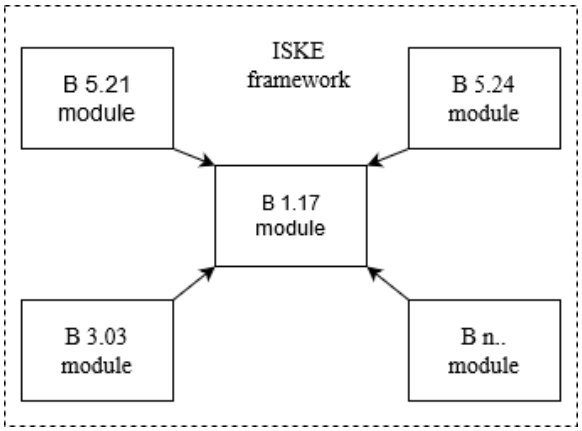

Figure 6 B 1.17 module dependency schema (Source: Author created)

3.3 Similarities between BSI C5 and ISKE B 1.17

3.3.1 Security Policies

The first similarities author noticed between the two frameworks are the importance of security policies and regulations including detailed documentation. This also includes the employees understanding of these policies. Author found that the topic of the policies range from ISKE G 2.1, G2.2 to G2.4 from shortcomings section and M 2.535 from implementation section. This in general matches the C5 SP Area. This is also a very obvious area for any security related framework.

3.3.2 Cryptography

The Concept of Cryptography is important to every cloud security framework since it ensures the authenticity, integrity and confidentiality of information. Cryptography ensures the transmission encryption of cloud customer data over the public network. It defines the latest and most secure cryptographic algorithms for usage. Ensures the usage of latest version of Transport Layer Security (TLS). Gives guidelines for public/private key management and describes possible attack vectors related to secrets, keys and certificates. Related controls are B 1.7 of ISKE and CRY from BSI.

3.3.3 Audit

Both frameworks define the guidelines for auditing and continuous audit. Rules for audits determine that an external specialist has to go to CSP at least once a year and verify that they still comply. This also includes possibilities to get certificates for complying with other standards such as ISO or NIST. Continuous auditing defines guidelines for operations processes such as making sure that logs are monitored and more.

3.3.4 Cloud Service Provider Contracts

Frameworks mention the Cloud Customer contracts with CSP's. This means data confidentiality and integrity contracts and CSP rules on access rights to customer data. [7] Any CSP contracts with third party and sub-contractors. Defined policies for termination of contracts between CSP and Customers. Ensuring data immediate deletion after termination.

3.4 Differences between BSI C5 and ISKE B 1.17

One of the clear differences was that ISKE has policy called "Creation of the Strategy for using Cloud service, M 2.534". It describes thorough analysis of economical, technological and security aspects even before the creation of the cloud service. [8] This control offers thorough analysis if it is beneficial to create cloud service or not. This also includes the Cloud service importance in the organization as a "whole". C5 just focuses on the implementation of the framework and not benefits strategy.

Author also notices that the B 1.17 emphasizes a lot on application and service part of the cloud which is handled by B 5.21 Web applications. It offers in-depth review of attack vectors such as SQL injection and authentication flaws form OWASP Top Ten and more. Where as the C5 wants the CSP to make their own analysis of potential threats and gives overall guidelines what to look into and analyse.

3.5 The Value of ISKE B 1.17

Overall the ISKE B 1.17 is a great framework that places great importance to detail, while the C5 focuses on the overall scope and requirements for each criteria. ISKE introduces many new categories such as:

- Potential technical difficulties
- Potential threats for the systems
- Potential human errors

All of these points are carefully planned out and described using examples giving the CSP who plans to implement ISKE more understanding of what policies and guidelines to document. The B 1.17 also has security level for each control such as L, M and H for the framework implementation part, so the CSP knows what kind of level to expect when implementing controls. [9]

As CSP is dealing with SaaS service model where customers use the web applications to access the cloud, the B 5.21 which the B 1.17 is dependent on describes the web application protocols and attack vectors very deeply. It gives a great overview of many threats and vulnerabilities which the C5 does not.

4 Practical result analysis

4.1 Organisation of Information Security (OIS)

Goal: The OIS deals with implementing information security management system (ISMS) within the organisation. An Information Security Management System describes and demonstrates your organisation's approach to Information Security. [10]

Conclusion: All of the criteria described in the OIS failed to comply since the company has not implemented any security frameworks or ISMS. Risk management system or policies related to it are non-existent.

The result of OIS criteria could be improved by implementing an actual ISMS or cloud security framework. The OIS-01 suggests looking at the ISO/IEC 27001 standards for more information. This would improve the CSP security level by huge margin and also allow it to comply with C5 OIS criteria and many more criteria from other areas.

Result: 0/7 of the criteria fulfilled

4.2 Security Policies and Instructions (SP)

Goal: This area defines the overall security policies and instructions made by the CSP for their cloud environment. This is also important for other areas and criteria that depend on the policies defined in the SP.

Conclusion: CSP fails to comply with all criteria in this area. Reason is related to the undefined and non-existent instructions and policies regarding cloud security. The SP is a base for many other criteria such as Operations (OPS) and prevent the CSP of offering best security in any area that depends on the policies defined in the SP.

The result of SP criteria could be improved with well documented security instructions and guidelines provided for all employees or implementing a security framework. Possibly implementing ISMS. This includes:

- Risk management
- Defining employee roles and responsibilities

- Security Strategy
- Review of defined policies

Result: 0/3 of the criteria fulfilled

4.3 Personnel (HR)

Goal: Employee awareness on information security and understanding their role and responsibilities in their organisation. This also includes the procedures after the termination of the employee contract.

Conclusion: Documentation and guidelines for any security awareness training is not defined. The employees of the CSP all have certain amount of self-taught security awareness, but have not gone to any training or possess any security related certificates.

The result of the HR could be improved documented disciplinary measures for the employees. Employees should also be sent to security training at minimum of every six months.

Result: 4/6 criteria fulfilled

4.4 Asset Management (AM)

Goal: Secure assets management of the organisation from acquisition and commissioning to decommissioning and disposal.

Conclusion: Cloud service scored very well in this area. The company has a good asset management system. Assets are documented and classified in the management tool called iTop. ITop is an Open Source web application for the day to day operations of an IT environment. [11] Acquisition of assets goes through review and planning. Disposal is handled by an experts. The CSP has well documented policies for employee hardware, software and malware scanner. Employees must verify their assets once a year.

Although CSP scored very well in this area with the base criteria, there are always additional criteria to be applied which offers more reliable security measures. The AM-01, AM-05 and AM-06 have additional criteria that the CSP does not comply with.

Result: 6/6 criteria fulfilled

4.5 Physical Security (PS)

Goal: Secure environment against unauthorised access and prevention of service outage in the premises where the cloud service is provided.

Conclusion: Cloud service scored decently in this area. Physical site of the servers is in secure datacentre in Telia. They have strict access to the server room and all racks are protected with locks to prevent any unauthorized access to hardware. Fire and smoke systems are implemented.

The main concerns in this area are the missing documentation regarding the requirements of physical environment security for the CSP. The second concern is missing redundancy for the cloud service. Currently there is no plan to implement redundancy for the service due to company being on a very small operation scale.

This area could be improved by well documenting the physical environmental guidelines and defining a redundancy model for cloud service.

Result: 5/7 sub-criteria fulfilled

4.6 Operations (OPS)

Goal: As the name of area says, it's for ensuring that operations of the cloud service run smoothly. Plans are implemented for monitoring, malware protection and irregular events such as malfunctions and failures.

Conclusion: Cloud service scored decently in this area. Most of the concern is due to missing documented policies and guidelines for the operations part. Also there are no procedures for regular testing of the operations. But most of the practical criteria are fulfilled. Company has good monitoring system called Zabbix. Zabbix is a mature and effortless enterprise-class open source monitoring solution for network monitoring and application monitoring of millions of metrics. [12] Zabbix covers most of the practical monitoring part of this area. Then there is also issue with the vulnerability and incident management which has not been documented by the CSP. But a part of it is also application side which Nextcloud covers with detailed documents.

Result: 17/24 criteria fulfilled

4.7 Identity and Access management (IDM)

Goal: Secure and correct authentication and roles for the users of cloud service.

Conclusion: There is some unmet criteria for this area. Most of it is due to missing documentations for the user rights management. There are policies and guidelines for regular access rights review and privileges. This also includes some password policies, user locking and deactivation due to inactivity.

This area could be improved by writing well defined user rights management policies. The user rights policies are actually something that should always be implemented whether actual framework is used or not. Since customer user rights should be well defined to prevent any trouble in the future with the legal side.

Result: 5/9 criteria fulfilled

4.8 Cryptography and Key Management (CRY)

Goal: To protect confidentiality, authenticity and integrity of the information using state of the art encryption and cryptographic mechanisms.

Conclusion: Cloud service scored well in this area. This is due to SaaS cloud service model. Where most of the cryptographic side is handled on the application side. Nextcloud is known for its security, it uses state of the art encryption techniques for securing information data during transfer process and also storing it.

The only downside in this was documentation. Since Nextcloud allows many encryption techniques we as a cloud service provider should document it and define the policy to use the latest and the greatest measures available.

Result: 3/4 criteria fulfilled

4.9 Communication Security (COS)

Goal: The goal of this area is the protection of information in the networks. This includes segmentation of administration and public cloud user networks.

Conclusion: The practical side of this area exists. Networks are well segmented and secured. Network topology is documented and monitored live with notifications if any irregularities happen. The criteria that is not met is related to the undefined and missing documentation of the CSP network policies and organizational safeguards.

To improve this area, well documented policies for CSP network should written.

Result: 5/8 criteria fulfilled

4.10 Portability and Interoperability (PI)

Goal: To allow customers access to the cloud service. This includes thing like contractual agreements of scope the CSP provides to the customer and procedures after termination of contract with the client.

Conclusion: The CSP failed in one of the criteria. Currently there are no documentation for interfaces. This could be improved with clearly defined documentation on interfaces.

Result: 2/3 criteria fulfilled

4.11 Procurement, Development and Modification of Information Systems (DEV)

Goal: The goal of this area is to provide information security for the development of the CPS' information systems.

Conclusion: In this are the Cloud Service Provider scored badly. This is also one of the debatable areas. Since the Cloud Service Provider outsources the technology used for the providing the cloud service. Author thinks that the development of application side criteria can also be filled by Nextcloud. The overall development of the information system using the application is the CSP's side.

To improve the unfulfilled criteria, the missing documentation of the development of the information system should be written, this includes risk assessment strategy of the development. Also one of the important points is to create a test environment to test any new configurations to the system. Currently there is only live environment for the customers.

Result: 1/10 criteria fulfilled

4.12 Control and Monitoring of Service Providers and Suppliers (SSO)

Goal: Security of the information that the subcontractors of the CSP can access and monitor.

Conclusion: The CSP also scored badly here, none of the criteria were met. Currently there are no subcontractors for the CSP, so such guidelines were never needed. Criteria were not met due to unwritten policies. This area is mostly about documented policies and strategies concerning the subcontractors. This could be improved by writing the policies specified by the specifications in the framework.

Result: 0/5 criteria fulfilled

4.13 Security Incident Management (SIM)

Goal: To manage and process security incidents.

Conclusion: The CSP did not do well in this area. Policies and guidelines for managing security incidents are non existent. The CSP only manages security incidents on the go, but does not follow any procedures regarding that.

This area could be improved by writing comprehensive guidelines and policies how to manage any security incident that may happen. This could also include setting up Community Emergency Response Team (CERT) consisting of few members who have adequate knowledge in the field of information security and are given responsibility to respond to such incidents.

Result: 1/5 criteria fulfilled

4.14 Business Continuity Management (BCM)

Goal: The goal of this area is managing the business side of security. It requires described policies of the security incident impact on the business continuity.

Conclusion: The CSP did not score well in this area. Policies for managing business continuity after the impact of a security incident are non existent. There is no testing or anything practical done to improve the area.

To improve this CSP has to build analysis policies and instructions for the business continuity. Do practical testing of the defined policies and continuously update and verify the policies and management plan.

Result: 0/4 criteria fulfilled

4.15 Compliance (COM)

Goal: COM deals with legal aspects of the cloud service. This ensures that monitoring, maintenance are done according to regulations. Managing regular audits.

Conclusion: Currently none of the criteria in this are fulfilled. All legal compliance documents are missing according to author.

To improve this area, CSP has to write legal compliance documents and regulations for the cloud service. Write legal policies for external audits.

Result: 0/4 criteria fulfilled

4.16 Dealing with investigation requests from government agencies (INQ)

Goal: Handle legal government investigations. Allow government according to the legal requirements review information to cloud customers and limit access to the data.

Conclusion: As far as author knows the policies for such actions have not been clearly defined yet, so all the criteria are non-existent. But even without the policies cloud customers can be informed of such legal investigations.

To improve this area well defined documentation has to be written to manage any governmental investigations on the premises of CSP and cloud customers data.

Result: 0/4 criteria fulfilled

4.17 Product Safety and Security (PSS)

Goal: Provide latest security updates and inform cloud service customers of the latest vulnerabilities. This also includes providing secure authentication and troubleshooting for cloud customers.

Conclusion: The result of criteria fulfilled in this area are good. Most of the criteria are met on the application side. Nextcloud is knows to always offer latest updates. Nextcloud also has cloud service security scan website where customer can enter the address of the cloud service and the scanner test cloud service for known vulnerabilities and latest patch and update levels. The few unmet criteria are the result of missing documentation and guidelines for customers on how to securely use the service. The second unmet criteria is related to the location of the data. Unfortunately, currently there exists only one option.

This area could be improved with defined documentation and having another redundancy/backup datacentre somewhere else.

Result: 8/12 criteria fulfilled, 2 not applicable to the SaaS service model

4.18 Conclusion of practical solution

The practical analysis gave us as a CSP very good overview of the security conditions related to our cloud services. Using the BSI C5 cloud security framework we were able to determine our missing security policies and regulations. The C5 framework was very good checklist tool for our case, since Nextcloud complies with BSI C5 and ISO 27001 standards. This helped us a little to separate some aspects of the outsourced application and our infrastructure using the C5 Catalogue.

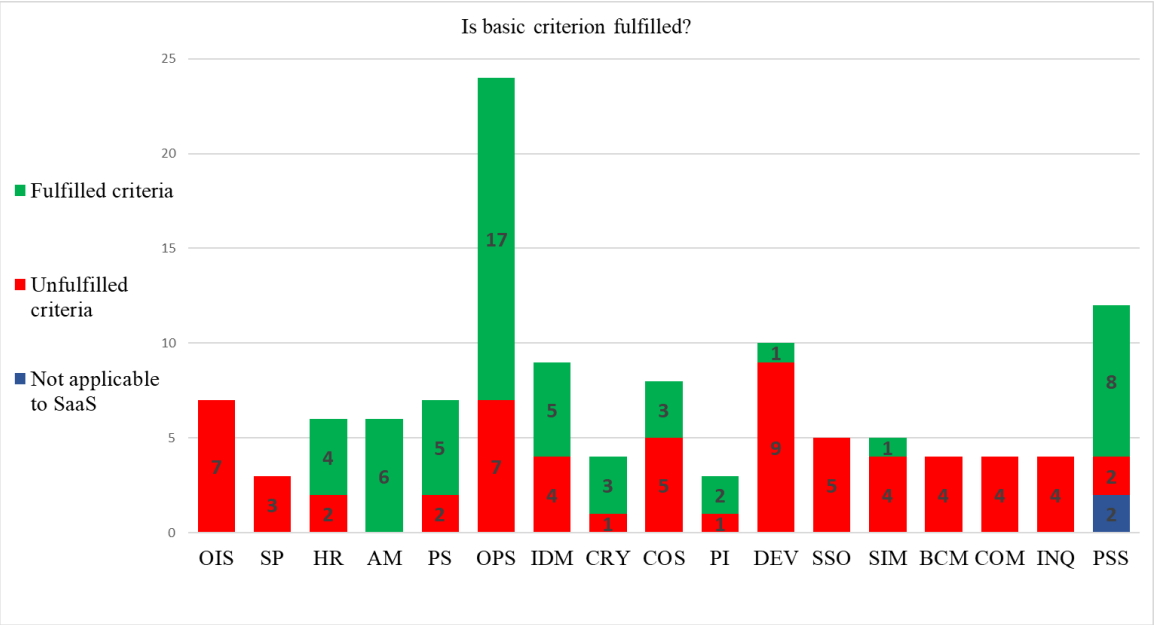

Figure 7 Statistics of the met and unmet criteria. (Source: Author created)

The Figure 7 gives a good statistical overview of the areas where the CSP has failed, where improvements could be made and what are the strong suite. Unfortunately 6/17 areas have completely failed to meet the standards. This is mainly due to missing these points:

- Information Security Management System (ISMS)
- Risk analysis management
- Any documented security policies for cloud service
- Security instructions for third parties and suppliers
- Business continuity management plans
- Legal and contractual policies for external audits

Most of the unmet criteria is to do with non-existent security policies and regulations. Fortunately there are some written policies and not all areas are failing. Asset management of the CSP is fully regulated. The CSP has a great asset management tool which has the ability to classify and label assets. Employees understand policies and regulations for safe-handling of company assets. CSP has good physical security of hardware and company assets. All the hardware and information systems are monitored

24/7 by the CSP. Nextcloud provides us information confidentiality and integrity by offering latest security for authentication and session management. Cloud customers data is encrypted in storage and during transfer.

Author has pointed out where and how CSP could improve cloud security standards. author also thinks that since the CSP complies with under half of the criteria in C5 (55/121), the CSP should think of implementing the BSI C5 module of the framework for improved security. Perhaps not only the C5 but the BSI security framework as whole.

5 Summary

The goal of this work was to compare two cloud security frameworks where one of the frameworks was based on the other. The mentioned frameworks are BSI C5 and ISKE B 1.17.

In the theoretical analysis author gave overview of the two frameworks, described the structures and how the controls of each framework depended on one another. Author also compared similarities and differences between the two and finally to find the value added by the ISKE B 1.17 which is based on BSI C5.

Based on authors analysis ISKE adds new things like more detailed controls, describes potential difficulties for the cloud, potential threats in more detail and describes possible human errors in cloud environment.

The practical goal of this work was to compare authors work cloud environment standards with the standards described in BSI C5 framework. C5 was chosen because of the certified compliance with the cloud platform that author used for his work.

Result of the practical work was a checklist of criteria compliances that were or were not met by the CSP. For the solution author did an analysis of practical work and gave suggestions in each area, how the CSP could correct and improve the standards.

References

[1] 10 critical cloud security threats in 2018 and beyond. [Online]. Available: https://www.synopsys.com/blogs/software-security/10-cloud-security-threats-2018/ [Accessed 10 April 2020]

[2] Three-level IT Baseline Security System ISKE. [Online]. Available: https://www.ria.ee/en/cyber-security/it-baseline-security-system-iske.html. [Accessed 1 April 2020]

[3] Nextcloud Compliance Kit. [Online]. Available: https://nextcloud.com/gdpr/. [Accessed 10 April 2020]

[4] What is different about cloud security. [Online]. Available: https://www.redhat.com/en/topics/security/cloud-security. [Accessed 1 April 2020]

[5] IT-Grundschutz-Standards/BSI-Standards. [Online]. Available: https://www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandards_node.html. [Accessed 2 April 2020]

[6] Cloud Computing Compliance Criteria Catalogue (C5) [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2020/C5_2020.pdf?__blob=publicationFile&v=1 [Accessed 14 April 2020]

[7] Choosing of cloud service provider [Online]. Available: https://iske.ria.ee/8_06//ISKE_kataloogid/7_Kataloog_M/M2/M_2.540 [Accessed 18 April 2020]

[8] Cloud service usage strategy [Online]. Available: https://iske.ria.ee/8_06//ISKE_kataloogid/7_Kataloog_M/M2/M_2.534 [Accessed 20 April 2020]

[9] ISKE B 1.17 Cloud services [Online]. Available: https://iske.ria.ee/8_06/ISKE_kataloogid/5_Kataloog_B/B1/B_1.17 [Accessed 21 April 2020]

[10] What is an Information Security Management System(ISMS)? [Online]. Available: https://www.isms.online/information-security-management-system-isms/ [Accessed 15 April 2020]

[11] What is iTOP [Online]. Available: https://www.itophub.io/wiki/page [Accessed 16 April 2020]

[12] Zabbix the enterprise-class open source monitoring solution. [Online]. Available: https://www.zabbix.com/ [Accessed 12 April 2020]

Appendix 1 – Practical work

Practical work of comparing BSI C5 with Cloud Service Provider:

https://drive.google.com/file/d/1QBl4YcrCXow1BtIQTNhcI78gQPvcEN5G/view?usp=sharing