Improving IT administration security by using security controls based on security frameworks

Leevi Hertteli

Master’s thesis
05 2022
Technology, communication and transport
Master’s Degree in Cyber Security

Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Hertteli, Leevi

Improving IT administration security by using security controls based on security frameworks

Jyväskylä: JAMK University of Applied Sciences, May 2022, 60 pages.

Technology, communication and transport. Degree Programme in Cyber Security. Master's thesis.

Permission for web publication: Yes

Language of publication: English

Abstract

Cybercrime continues to grow, and more effort should be put into defending capabilities against criminals. When an attacker breaks into an organization's IT infrastructure, its primary goal is to reach the administrator's desired maintenance credentials that would allow them to gain access to critical assets and sensitive information. This could lead to a significant compromising of core business operations. The idea for the chosen topic arised from my own work and experiences that have been over the years of IT maintenance work. Each activity involves threats and risks and therefore, efforts are constantly made to examine one's own activities at work, e.g. how the daily tasks are safely performed without compromising the organization's operations.

A constructive method was used as a research method in the study. The purpose of the development research is to focus solely on enhancing information security related to IT maintenance. The work creates and develops a risk management tool that is used in workshops as a tool for risk analyses. The goal is to find the necessary development targets and controls to improve the security of IT maintenance through risk assessment. The research aims are exploring different kinds of IT security criteria and standards to find recommendations and controls, and to mitigate the risks identified in workshops. Another key part of the work is to identify the protectable assets and threats.

During the implementation phase of the work, the current state analysis of the IT management was created based on queries and observations. The most important part of the implementation was to organize workshops for IT department personnel, where all the main steps involved in risk assessment were re-viewed. Assets and threats were identified, risk levels were assessed, and controls were discussed to mitigate risks. The workshop's outputs were used as research material in this work.

To serve the organization, a risk management tool was developed to help assess risks and maintain security management. In the workshops, a lot of assets and threats were identified and those were examined more detailed in the risk analysis. The results of the risk analysis show that most of the risks assessed are intolerable risks. The reason for this is certainly because the workshop focused on better understanding of where most critical risks arise from and how the risk could be reduced.

Keywords/tags (subjects)

Administrative privileges, Frameworks, Security controls, Security criteria

Miscellaneous (Confidential information)

Some of the contents of Appendices 1 and 3 are confidential and removed from the public thesis. The basis for secrecy is section 24(17) of the Act on the Openness of Government Activities 621/1999, a company's business or trade secret. The period of secrecy is five (5) years, the secrecy will end on 18 May 2027.

Hertteli, Leevi

Improving IT administration security by using security controls based on security frameworks

Jyväskylä: Jyväskylän ammattikorkeakoulu, toukokuu 2022, 60 pages.

Tekniikka ala. Tieto- ja viestintätekniikan tutkinto-ohjelma. Opinnäytetyö YAMK.

Verkkojulkaisulupa myönnetty: Kyllä

Julkaisun kieli: englanti

Tiivistelmä

Kyberrikosten määrä jatkaa kasvuaan ja panostuksia puolustuskyvykkyyden nostamiseen rikollisia vastaan tulisi laittaa entistä enemmän. Yritysten IT-infraan murtautuvan hyökkääjän ensisijainen tavoite on päästä käsiksi ylläpitäjän halussa oleviin ylläpitotunnuksiin, joiden kautta hyökkääjälle avautuu pääsy kriittisiin järjestelmiin ja arkaluontoisiin tietoihin. Tämä voi johtaa siihen, että yrityksen ydinliiketoiminta vaarantuu merkittävästi. Tutkimuksen aihe löytyi omasta työstä ja kokemuksista, joita on kertynyt vuosien ajan IT-ylläpitotyössä. Kaikkeen toimintaan liittyy uhkia ja riskejä. Tämän vuoksi omaa toimintaa tulisi tarkastella ajoittain, jotta tiedostetaan, kuinka päivittäiset tehtävät voidaan suorittaa tietoturvallisesti vaarantamatta organisaation toimintaa.

Työssä käytettiin konstruktiivista tutkimusmenetelmää. Kehittämistutkimuksessa keskityttiin pääosin IT-ylläpidon tietoturvan kehittämiseen. Työssä kehitettiin organisaatiolle soveltuva riskienhallintatyökalu, jota myös käytettiin työpajoissa riskien arvioinneissa. Tavoitteena oli löytää riskiarvioinnin kautta tarvittavat kehittämiskohteet ja kontrolleja IT-ylläpidon tietoturvan parantamiseksi. Tärkeä osa työtä oli myös tunnistaa suojattavat kohteet ja niihin kohdistuvat uhat.

Työn toteutusvaiheessa luotiin tilannekuva IT-hallinnasta kyselyjen ja havaintojen pohjalta. Keskeisin osa toteutusta oli järjestää tietohallinnon henkilökunnalle työpajoja, joissa käytiin läpi riskien arvioinnin tärkeimmät vaiheet. Prosessin aikana tunnistettiin suojattavia kohteita, uhkia ja arvioitiin riskien suuruuksia sekä mietittiin kontrolleja, joilla riskejä voidaan vähentää. Työpajan tuotoksia käytettiin tutkimusmateriaalina tässä työssä.

Työpajoissa tunnistettiin useita suojattavia kohteita ja uhkia, joita otettiin tarkempaan käsittelyyn riskianalyysissä. Suurin osa analysoiduista riskeistä arvioitiin erittäin vakaviksi riskeiksi. Työpajoissa keskityttiin analysoimaan, mistä kriittisimmät riskit aiheutuvat ja millä keinoilla riskejä pystytään vähentämään. Kehitettyä riskienhallintatyökalua voidaan jatkossakin käyttää apuna riskien arvioimisessa ja tietoturvan hallinnan ylläpitämisessä.

Avainsanat (asiasanat)

Järjestelmänvalvojan oikeudet, viitekehykset, turvallisuus kontrollit, turvallisuus kriteeristöt

Muut tiedot (salassa pidettävät liitteet)

Liitteet 1 ja 3 ovat osittain salassa pidettäviä, ja ne on poistettu julkisesta työstä. Salassapidon peruste on julkisuuslain 621/1999 24§, kohta 17, yrityksen liike- tai ammattisalaisuus. Salassapitoaika on viisi (5) vuotta, salassapito päättyy 18.5.2027.

Contents

Figures

Tables

1 Introduction

1.1 Thesis Scope and Goals

Purpose of the thesis is to explore different kind of IT security criteria and standards and to find out security controls, best practices and hardenings to mitigate or remove the threats and risks that affect the function and maintenance of IT administration.

The goal of this work is to improve the security of IT maintenance by using various security criteria and standards and other good practices. In practice, the rules should be established for how the IT infrastructure management is securely managed by technical and administrative methods, whether working remotely or from the office.

The idea for the chosen topic is on my own work and experiences. Each activity involves risks and threats and therefore, efforts are constantly made to examine one's own activities at work, e.g. how the daily tasks are safely performed without compromising the organization's operations.

This study is useful for all in-house operators and certain IT house operators who provide the IT support and system maintenance as an outsourced service to different organizations. The purpose of this study is to map the security controls and requirements of the different criteria related to IT management as widely as possible. In addition, the purpose of this study is to find out ways of how to carry out IT management securely through processes and technical methods.

It is important to examine this issue because it is dealt with comprehensively in this study, taking into account all the hard-core criteria and starting from the premise that aim is to keep the subject dealt with only in the context of the IT management.

1.2 Host company

Aava Medical Centre is a Finnish family-owned company that has been promoting health and well-being for over 50 years. The family business employs more than 1300 professionals. Aava offers general practitioner and medical specialist services that include more than 40 medical specialties. Occupational health-care takes care of the ability of 110 000 employees. Aava has 19 clinics in Finland. The company wants to take responsibility for the well-being and health of its customers, not only to treat illnesses, but also to take care of their health and well-being in their everyday lives.

1.3 Cyber security threats

In this work, the topic is dealt solely from the point of view of IT maintenance. IT maintenance has access to critical systems and data in the organization, which means that the need for security controls is greater than that of a standard user who works in another role in the organization, e. g. as a financial administration employee or doctor. (National institute of Standards and Technology 2020, 342.)

According to Verizon Data Breach Investigation report (DBIR) in 2021, it was mentioned that errors caused by a system administrator have decreased during COVID-19 pandemic. However, it was reported that ransomware type attacks have almost doubled in amount. Ransomware attack has increasingly become a new dimension not only in the encrypting of information, but also in publishing data that contain ransom demands. In addition, the phishing and social engineering campaigns and use of stolen credentials have been growing in the past year as shown in **Error! Reference s ource not found.** (Verizon 2021, 16) and the most common types of the breaches that have occurred during the covid pandemic are presented in Figure 2. (Pescatore 2021, 4)

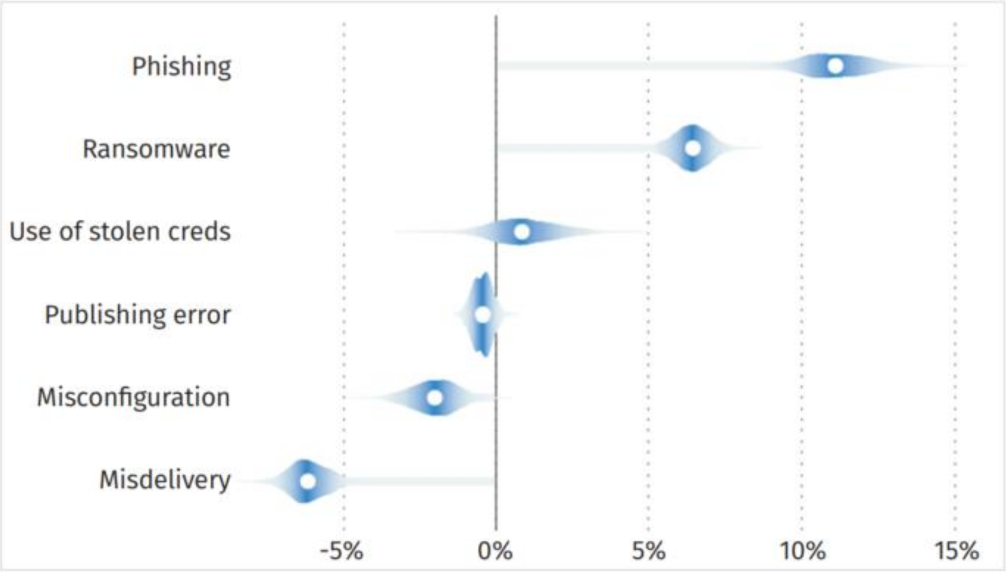


Figure 1. Shows the types of attacks that have occurred in the past year.

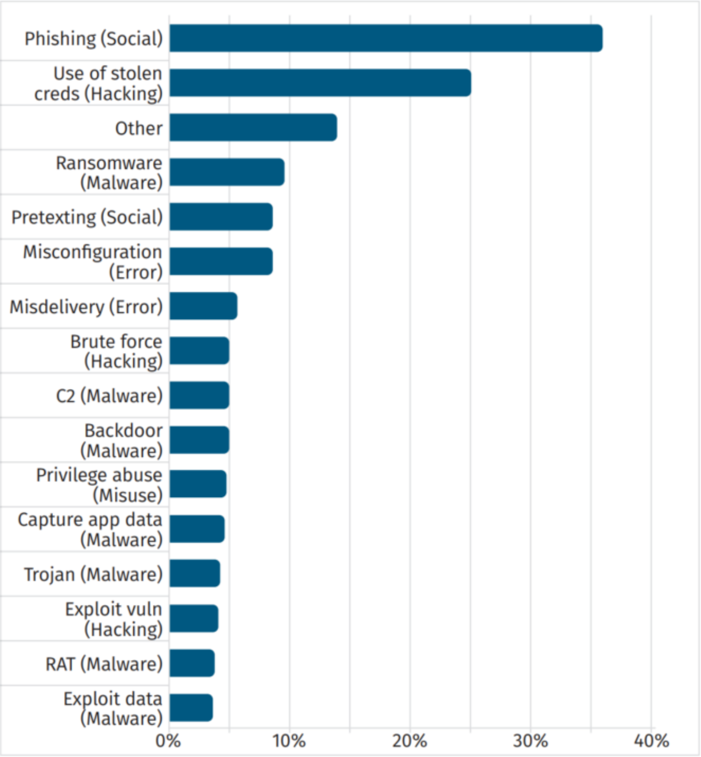
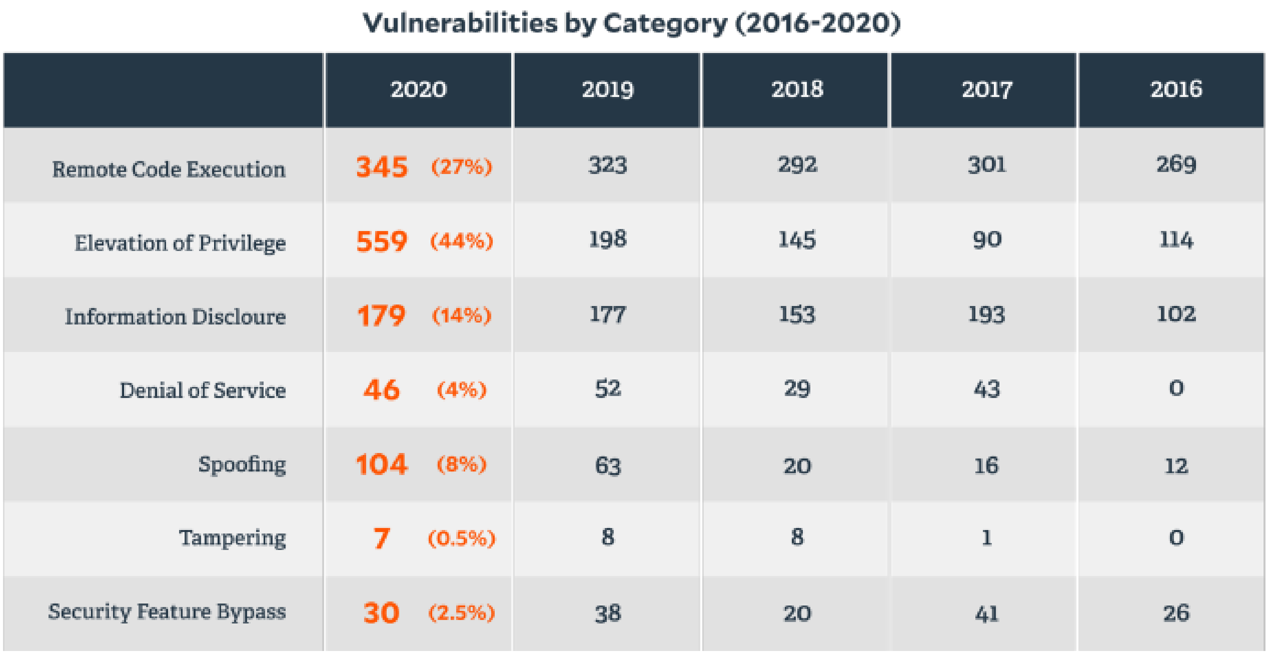


Figure 2. Top action varietes in breaches.

According to Microsoft's report, the number of critical vulnerabilities has levelled off, but overall the number of vulnerabilities has been increasing over the last five years. The report points out that 56% of critical vulnerabilities can be mitigated by removing admin permission in 2020. Figure 3 (BeyondTrust 2021, 9.) illustrates that vulnerabilities in elevation of privilege category have been growing sharply between 2019 and 2020, the number has increased almost threefold in one year. (BeyondTrust 2021, 9.)



Vulnerabilities by Category (2016-2020)

	2020	2019	2018	2017	2016
Remote Code Execution	345 (27%)	323	292	301	269
Elevation of Privilege	559 (44%)	198	145	90	114
Information Discloure	179 (14%)	177	153	193	102
Denial of Service	46 (4%)	52	29	43	0
Spoofing	104 (8%)	63	20	16	12
Tampering	7 (0.5%)	8	8	1	0
Security Feature Bypass	30 (2.5%)	38	20	41	26

Figure 3. Vulnerabilities by category.

1.4 Research process

This study includes five main steps, which are organising a questionnaire for IT department, evaluating the current IT security state by carrying out a query, establishing own controls set from the controls of the most well-known criteria, organising a workshop and finally, comparing the results of the workshop with existing standards and the previously established own criteria. The phases of the research process are described in Figure 4.

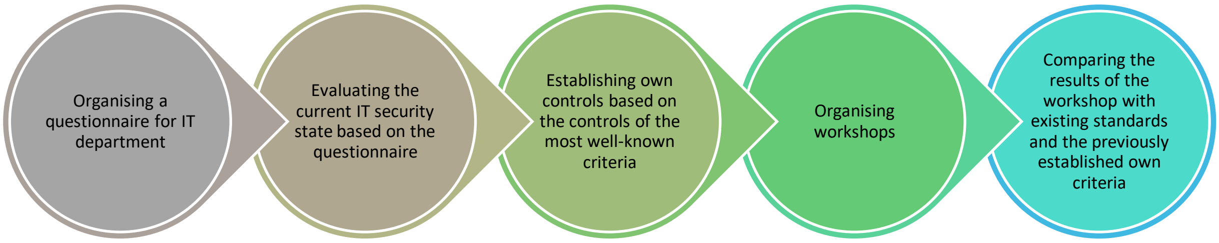

Organising a questionnaire for IT department
Evaluating the current IT security state based on the questionnaire
Establishing own controls based on the controls of the most well-known criteria
Organising workshops
Comparing the results of the workshop with existing standards and the previously established own criteria

Figure 4. Research process phases.

In the first phase, questionary is to be arranged to staff for an analysis of current IT security state. The aim is to get as comprehensive picture as possible of IT management practices. The questions are intended to clarify how maintenance tasks are performed and in what way. The questionary serves as a good tool for preparing a workshop that is organized for colleagues to identify as many threats to IT administration and its assets as possible.

Security controls related to IT administration and functions, such as systems and network management, are collected as widely as possible from different criteria and standards. Several criteria are included in the study, as the topic has been significantly limited to ensure that controls can be collected as extensively as possible from the topic area under discussion. There may be criteria that do not take very comprehensive account of security controls related to IT administration. A plan is then created to enhance and harden the environment.

Based on this query, an overall picture of current IT management is created. The questions are intended to clarify how the maintenance tasks are performed.

In the workshop, threat analysis is created by using the scenario method. In practice, author of the thesis organizes workshops for colleagues to identify as many threats to IT administration and its assets as possible. Threats are to be mapped through scenario brainstorming within the team of colleagues. Once the threats have been mapped, the most critical threats will be taken into closer consideration. Risk analysis is performed on threats and their consequences and impacts are discussed and documented. After the risk analysis, controls shall be selected for the target to be protected, to reduce the risk and then the risk analysis is re-performed. This shows how much the control has reduced the risk. The results of the risk analysis can be compared between current and after control effect, which also determines the residual risk.

A risk analysis is created for IT administration and different types of management connections. The risks related to e.g. remote working, are assessed. An acceptable risk level is assessed. If it is stated that the risk is too high, measures and improvements to mitigate the risk are needed. Through risk assessment it is easier to justify the actions required, and some actions may also require a financial investment. Requirements for risk mitigation are set. The effects are outlined and described if the risk materializes, for example, as a monetary estimate.

After the workshop, results of the query and workshop are mirrored and compared against the controls found in the different frameworks, standards and the team's own controls. A plan is then created to enhance and harden the environment. As a result of above-mentioned phases, research data is obtained for the thesis.

The goal of the research is simply to create the design of measures, but technical implementation is not carried out. However, there are good capabilities and conditions for technical implementation later on if seen necessary. Although technical implementations are not carried out during the work, the functionality of the controls and the reliability of the results are ensured by relying on the competences of the experts participating in the workshops, and the specific recommendations of the various criteria. The controls and measures required for many information security problems evidently measure the risk. It is not only technical solutions that can repair the shortcomings, but also through process changes, instructions and way of acting can lead to significant improvements in raising the maturity level of information security.

Several criteria are included in the study, as the topic has been significantly limited to ensure that controls can be collected as extensively as possible from the topic area under discussion. There may be criteria that do not take very comprehensive account of security controls related to IT administration.

1.5 Research-Method

Constructive research was chosen as the approach to development work. This approach is suitable for this type of a project, where it is intended to make a plan and create a model based on which the desired solution can be implemented, and which may improve the current practices. Through constructive research, a theoretically grounded solution that produces new information for the organization is produced. In addition, constructive research is also suitable because the project is intended to make changes in the way of operation. Practices and solutions are changed based on theoretical information. Constructive research can be used for solving a genuine practical problem where an organization's operations and procedures are changed. This research perspective is appropriate when theoretical knowledge is needed for problem-solving. For research purposes it is necessary to scientifically prove what security controls and methods are required to improve the information security situation. In constructive research, different methods can be used freely, and the collection of the data can be carried out in several ways. (Ojasalo et al., 2015, 65-66,68)

According to Lukka (2014), constructive research is a method for solving practical problems. New innovative constructions are created and valuable material for the field of science is produced. Construction refers to an abstract concept: plans, information system models, commercial products, organizational structures, and outputs created by innovators. In constructive research, it is essential to focus on the practical problems that are being faced in the challenges of life that need to be solved. Innovative solutions that ultimately solve the core problem can be achieved, including those steps that ensure the suitability and functionality of the construction in practice. Another essential part of the research approach is that close cooperation is performed between the research and practical representatives, who create learning experiences for different parties. In addition, constructive research strongly based on theoretical knowledge and applies empirical findings back to theory. The following steps are included in constructive research:

1. Find a practically relevant problem
2. Obtain an understanding of the topic and the problem
3. Innovate, i.e., construct a solution idea
4. Demonstrate that the solution works
5. Show theoretical connections and research contribution
6. Examine the scope of applicability (McGregor, 2018.)

Firstly, a valid subject or a problem to be investigated and solved needs to be recognized. The problem that is handled in study is thoroughly reviewed from a practical and theoretical point of view. The second step is to study the topic and to understand the problem in depth and to get the most comprehensive overview of the baseline. This can be called field research and different methods for collecting material such as interviews, observations, and analysis of written materials can be used. (Lukka 2014.)

In the next phase, a solution model will be innovated, and a construction will be developed to solve the problem. It is the most critical step in the whole process, because it shows whether the project can be moved on or not. Innovative construction development is helped by close cooperation between practical representatives and researchers. It can produce a fruitful outcome by combining practical and in-depth theoretical knowledge. After innovation, a solution is created, and its functionality is tested. Getting to this stage should not be taken as a given. It is not only enough to find a technically viable solution, but also necessary to verify the functioning of the research process. At this stage, the cooperation between the researcher and the practical representatives will become even more important, as the innovation and development of the structure must also be carried out by convincing the various parties and stakeholders through guidelines, trainings and pilot tests. (Lukka 2014.)

The advantages of a constructive research approach are that it provides an opportunity to bring researchers and target organisations to cooperation. At the same time, it also creates a strong partner and ability to solve the problem on the basis of thorough analysis and work. In turn, the risks of the research approach may be that the cooperation between the parties does not work and is not actively maintained. The risk may be that the significance of the problem to be investigated for the researcher is not sufficient. At the beginning of the project, it is important to analyse carefully and critically the significance of the practical problem between the parties involved. From the point of view of the target organisation, the concern may be that the objectives originally set in this case will not necessarily be wasted in vain. (Lukka 2014.)

The study will not be able to verify how the selected solutions and plans work in practice. The practical part is excluded from the work. However, the validity and suitability of the solutions can be prejudged on the basis of the fact that some of the controls come directly from the laws, regulations, criteria and standards, which have carefully been selected for a particular purpose. There has been a thorough analysis of the criteria by the expert working group and the assessments and recommendations they have drawn up can be relied upon. (Lukka 2014.)

1.6 Main research questions

The key topics handled in this research are mapping the control of the criteria and developing an appropriate risk management tool for the organization. The goal of the research is to find the answer to the following questions:

- Are there any ready-made controls in the existing security frameworks?
- Did significant risks detect during the risk analysis?

1.7 Previous research

This thesis handles several topics, and several research was found dealing with some of the same topics, but no exactly same approach was found.

Antti Kuokkanen from JAMK has been studied PAM topic in his master's degree thesis, which is centrally related to administrative management as a whole and the main idea of the thesis was to focus on managing privileged rights and safeguarding them. The output of the work serves as a guide to PAM topic for a first-timer. A model for performing the management of high rights and describing how PAM should be implemented in practice and what components are included in the whole is presented in his work. The technical details were not highlighted in the work, but they were excluded from the work. (Kuokkanen 2020.)

Tuomo Leppänen from JAMK has been done thesis with a topic of Practical implementation of Windows end-point security controls in his master's thesis. Several elements that can harden and safeguard the function environment of administration management have been taken into account in the work. KATAKRI criteria have also been introduced as a tool to obtain requirements and recommendations. Leppänen built proof-of-concept solution that faced the KATAKRI requirements. The work focused on the requirements of technical information security and approached the topic from the point of view of workstations. The work brought concrete methods and security controls to improve the defence capability on the IT management side. (Leppänen 2017.)

Rusere and Ernest from University of South Africa have written an article which topic is A Preliminary Network Security Framework for Tertiary Institutions. The study has established and developed a security criteria that enables capability for the institution to secure the entire network infrastructure by using innovative Information Technology techniques in accordance with the strategy they have set. Institution’s common network security challenges and threats are identified and mapped. The study has included well-known criteria for handling such as COBIT, ISO 27001 and NIST, which enable cyber-security risks and security threats to be managed and mitigated. The study launched a framework that consists of seven phases: Zero Trust, Plan, Secure, Privacy, Monitor, Incident and Report. The study emphasises the need to identify risks and threats in order to determine proportionate measures to mitigate them. Different perspectives are taken into account on a large scale, using the advice of the criteria, in order to effectively improve the institution’s cybersecurity defence capabilities. (Rusere & Ngassam, 2021)

This study differs from others by compiling its own controls based on several criteria related to IT security. In practice, a control list will be created, and it will be used to improve cyber security in remote connections and IT management. In addition, it is examined how cyber security is taken into account in the next thematic areas that serve as a framework during the thesis: network infrastructure management, remote management, segmentation, logging and monitoring.

2 Theory

2.1 Criteria

The study included two national Katakri and Pitukri as well as four international CIS, NIST, ISO 27001, PCI DSS security criteria for processing. Each criterion has its own emphasis, PCI DSS is strongly geared towards payment authorities, Katakri is used by the government officials to assess partners or companies operating for them whereas Pitukri is more aimed at cloud service providers. CIS is a very technical criterion. ISO 27001 is a strong policy and risk-based criteria and NIST is the broadest criterion of all. A very comprehensive set of criteria for significantly improving the information security of companies through controls is available. Although the criteria are intended for use by a particular sector, those can and should be applied to each sector of the organisation or regardless of the size of the company. Part of the criteria is very extensive, so there is a need to prioritize the scope to be studied. NIST alone contains about 900 security controls. For controls, the following topics shall be reviewed: IT administrative operating models, network infrastructure management, identity management, access management, remote management, segmentation and logging/monitoring.

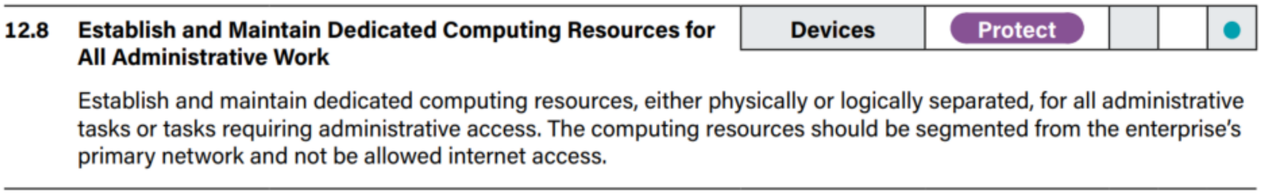
2.1.1 CIS

The Center for Internet Security is a technical benchmark that contains best practices, standards, guidelines for a sector of IT systems and product. The CIS framework consists of 18 critical security controls. In addition, this framework provides instructions on which configurations and settings are required to improve cybersecurity and helps protecting against internal and external cyber threats. In addition, CIS provides detailed instructions for a variety of products and systems, such as server software, operating systems, and network devices. (Sans Institute, 2021)

Network infrastructure management

Controls 12.3 and 12.8 emphasise that all administrative work should be carried out and managed using safe methods and tools and, in addition, safe network protocols such as SSH and HTTPS. First of all, the management of systems and network equipment should be carried out from dedicated platforms or out-of-band networks, physically or logically separated. The aim of this control is to ensure that maintenance is completely isolated from the production network by means of segmentation measures, and as a requirement, connections to the internet from the management machine are also prohibited. This requirement applies to all administrative tasks or tasks that require administrative access. (Center for Internet Security 2021, 40-41)

CIS also clearly takes the needs of IT system operators into account. One strict requirement is to implement security managing environment where the administrator performs administrative tasks by using different tools. Requirement 12.8 mentions and prompts administrative tasks to be performed dedicated platform that is separated physically or logically, as seen in Figure 5 (Center for Internet Security 2021, 41). It means that performing administrative tasks on dedicated computer is necessary. The IT administrator's computer should be separated from product environment and browsing on the web is disallowed. (Center for Internet Security 2021, 41)



12.8	**Establish and Maintain Dedicated Computing Resources for All Administrative Work**	**Devices**	Protect			●

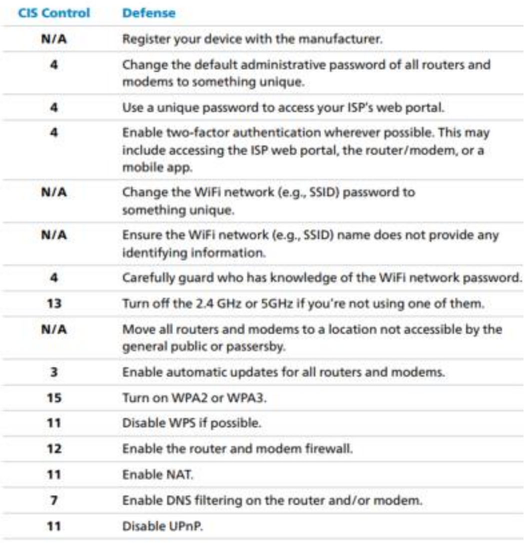
Establish and maintain dedicated computing resources, either physically or logically separated, for all administrative tasks or tasks requiring administrative access. The computing resources should be segmented from the enterprise's primary network and not be allowed internet access.

Figure 5. CIS control 12.8.

Remote management

Security configurations is to be ensured and the security profile should be scanned when a user connects to the internal network. Moreover, two-factor authentication is required for all the users who are allowed to remotely connect to the internal network. (Rapid7 n.d., 16)

Remote work has been on the rise considerably in recent years, and the company's systems and data are ever more managed through the home network. The company may not know what kind of home network equipment is used and how it is configured and whether sufficiently valid configurations are used. There may be low-quality home devices for consumers or small organizations, which may have default settings on and limited security functionality available. However, devices in the home environment face exactly the same kind of threats that occur in the most standard and robust devices or larger organizations. The most common threats are spying on browser usage and web activities, compromising connected devices and exploiting router's vulnerabilities. Among other things, neighbours, other people in the immediate vicinity of the home office and potential remote attackers on the network are seen as threat actors to data security. The defence capability and situation can be significantly improved by introducing security settings for the remote work recommended by CIS framework as shown in the Figure 6 (Center for Internet Security n.d., 23). There is also a marked control identifier to which each configuration is associated. (Center for Internet Security n.d., 23)



CIS Control	Defense
N/A	Register your device with the manufacturer.
4	Change the default administrative password of all routers and modems to something unique.
4	Use a unique password to access your ISP's web portal.
4	Enable two-factor authentication wherever possible. This may include accessing the ISP web portal, the router/modem, or a mobile app.
N/A	Change the WiFi network (e.g., SSID) password to something unique.
N/A	Ensure the WiFi network (e.g., SSID) name does not provide any identifying information.
4	Carefully guard who has knowledge of the WiFi network password.
13	Turn off the 2.4 GHz or 5GHz if you're not using one of them.
N/A	Move all routers and modems to a location not accessible by the general public or passersby.
3	Enable automatic updates for all routers and modems.
15	Turn on WPA2 or WPA3.
11	Disable WPS if possible.
12	Enable the router and modem firewall.
11	Enable NAT.
7	Enable DNS filtering on the router and/or modem.
11	Disable UPnP.

Figure 6. Security settings for remote work.

Control 12.7. prompts VPN solution is required for remote machines when connecting to in-company services. User authentication has been required to implement a solution that can prioritize accesses to enterprise resources on standard-user machines. (Center for Internet Security 2021, 41)

Security configurations is to be ensured and the security profile should be explored when a user connects to the internal network. Besides, two-factor authentication is required for all the users who are allowed to remotely connect to the internal network. (Rapid7, 16)

Segmentation

According to the cis guide, the ideal situation would be for the network to be separated so that the assets at the same sensitivity level are on the same subnet and thus separated from the company's assets that included different sensitivity levels. (Center for Internet Security 2021, 28)

Control 12.2 that refers that the principles of least privilege to be implemented in the segmentation. That means that if host, service or network is not a legitimate reason to communicate with second host, service or network, then it is not acceptable. In situations where services need to communicate with each other, only those ports or protocols that are needed for connections are allowed, others are blocked. The principle achieves the minimal need for user privileges and significantly improves safety and reduces the attack surface in the organization's environment. (Australian Cyber Security Centre, 2012.)

Rapid7's paper makes a good point about how segmentation should be considered. The first task to do is to stop and think about what the most critical assets in the organization are. Secondly, it should be considered whether there is a data classification policy in the company. In addition, it is necessary to think about who determines the criticality of the system and information. An organization-wide data classification policy should developed and applied it to all IT systems. The paper suggests using three classification levels: public, internal and confidential data. Public data is freely available and openly shared. Internal data is not intended for public use and confidential, sensitive data can affect the functioning of the organization if revealed. Based on the data classifications of the different IT systems, segmentation can be performed by placing IT systems in different VLANs with firewall rules. (Rapid7, 18.)

Logging and monitoring

Control 13.1 calls for all security event management of the company’s assets to be centralised in the same place where alerts can be set for various security events. The requirement is to implement a SIEM solution that enables vendor-based event correlation alerts. (Center for Internet Security 2021, 43)

The command line is usually used to get its driven malicious code in target, and there is also an opportunity to proceed in the network environment laterally. Control 8.8 prompts, all the management tools which administrators are used in the systems management such as powershell, bash and remote administrative interfaces. With the introduction of this control, the organisation has the ability to track and monitor the attacker’s footprints. (Shamma 2018, 44)

2.1.2 NIST CSF

NIST Cybersecurity Framework is a security tool that contain guidelines, standards, best practice and recommendations that can be used to organize and improve an organization’s cybersecurity. Through the implementation of recommendations and standards, the organization is thus more capable and prepared to identify and detect cyber-attacks, and the guidelines provide capabilities to respond, prevent and recover from cyber incidents. The criteria are published by the US National Institute of Standards and Technology. (Balbix, n.d.)

Network infrastructure management

Control SC-2 requires primary network user functionalities to be isolated from system management functionalities by physical or logical implementation. System activities include tasks that a system expert performs on a daily basis, such as managing databases, network components, workstations and servers. Several different means can be used to meet this requirement, such as using different workstations, versions of operating systems, centralized processing platforms or using a different network address i.e. using virtual technology or combinations of proposed methods. The isolation of systems and user functionalities can be performed by isolating admin interfaces by using additional domain access controls. There is also a requirement for the visibility of management tools to be prevented by standard users. (National Institute of Standards and Technology 2020, 293)

Remote management

More security controls need to be applied on remote work equipment because they face more threats, such as malware, device loss or theft, than enterprise environment devices. However, remote machines should contain the same security controls used in non-telework devices and additional security controls are recommended. When working remotely, the external environmental threats are greater compared to organization's local environment, so updates to operating systems and applications should be performed without delay, unnecessary services and ports should be disabled and the use of antivirus and host firewall is essential. Additional controls could be used to protect the sensitive data on the device and the existing controls can be adjusted. The organisation's mission would be to ensure that all types of remote devices are protected by properly referred solutions including PC, mobile phones and PDAs. The organisation must ensure that system administrators and users with a responsibility to secure telework devices have sufficient capabilities to secure them. (Scarfone et al., 2009, ES-2)

Each user should have a separate user account with limited privileges when using the PC remotely. Daily work is performed using a limited privilege account and separately used management IDs for administrative tasks with specific admin level access requirements. (Scarfone et al., 2009, 4-3)

Segmentation

Network security can be enhanced by segmenting networks not only for safety reasons, but also for network performance and controlled network broadcast traffic. Segmentation can also be used to manage and reduce visibility from hostile actor's perspective. (Rusere & Ngassam, 2021, 7)

In organization's IT infrastructure protection, network segmentation is one of the most significant and effective methods to impede a hacker's ability to cause damage to the organization's domain functionalities. Besides, the main idea is to secure the organization's operations to operate effectively by minimizing access to sensitive information. (Stouffer et al., 2015, 5-1)

The approach can be adopted by using the principles of least privilege and need-to-know. The main idea of these principles is that if there is no need for communication between certain systems, the communication is not allowed. (Stouffer et al., 2015, 5-2)

Before segmentation is carried out, operational a risk analysis needs to be carried out to specify the critical parts of the network infrastructure. Segmentation aims to get the network divided into smaller networks. (Stouffer et al., 2015, 5-1)

Logging and monitoring

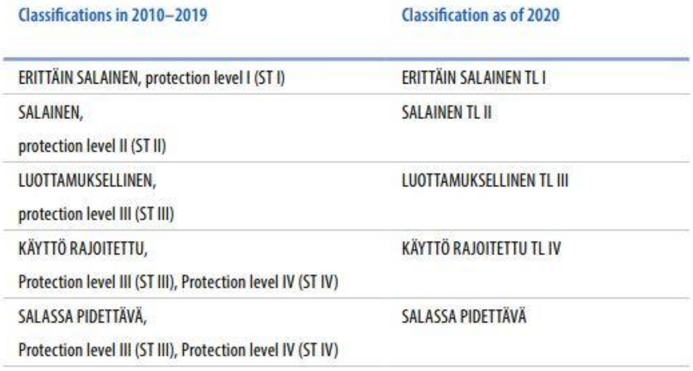
Control SI-4 requires enhanced monitoring of privileged users because they have access to critical and security-related data that standard users do not have access to. At worst, this can lead to a situation where a privileged user can cause worse damage to systems and organizational function than standard users. Enhanced privileged user monitoring can improve the ability to observe and enable malicious activity to be identified in good time and appropriate countermeasures can be used against them. (National Institute of Standards and technology 2020, 342)

Protecting network architecture requires intrusion prevention systems (IPS) that detect and prevent unprecedented network traffic and security issues such as insider threats. In addition, there needs to be an intrusion detection system (IDS) in the network boundary. It acts as a software or device and malicious and suspicious activities are detected in the network. One of the most important components of a network boundary is next-generation firewall that can contribute to mitigate data breaches with predefined rules to regulate and monitor network activities and traffics. (Rusere & Ngassam 2021, 7)

Perception capability can be improved by using different network monitoring tools or software such as Network protocol analysers, Network Taps, Port mirroring, Switch Port Analyzer, Threats intelligence devices, Simple Network Management Protocol (SMTP), Security Information Event Management (SIEM) and mobile device management (MDM). It is important to identify and know how the network being managed usually behaves, thus the operations of the network need be monitored regularly. In the event of attacks, threats, anomalies, they are much easier to identify and alarm limit values for situations are easier to adjust to SIEM. Possible attacks can be prevented by measuring in advance by performing vulnerability scans regularly to detect the most vulnerable assets. Vulnerability scans can be used to establish a current state of the assets in the environment in terms of upgrades. Vulnerability scans can also be used to assess the security risks and prioritise the repair of critical assets. (Rusere & Ngassam 2021, 8)

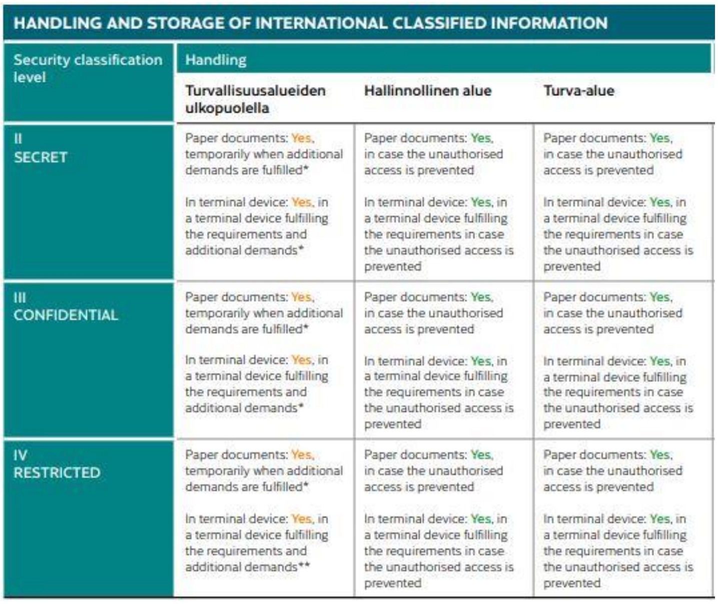
2.1.3 KATAKRI

Katakri is information security auditing tool for authorities. First version is published in 2009 and a latest version is in 2020. Nowadays, National Security Authority is responsibility maintaining and managing of Katakri. Through this auditing tool can test capability of organization to protect sensitive information. Katakri is a like check list for organization that can improve functionalities and securing information significantly, through that also can check what things already noticed. Katakri is compiled minimum requirements that based national regulations and international obligations. Katakri can use as auditing tool to evaluate the company’s security arrangements in a security survey. In addition, it can be used as an aid to companies, communities and different kind of organizations in security tasks and it is development. In Katakri, secrecy and security classification levels are determined as shown in Figure 7 (Ministry of Finance 2021, 19). The more detailed handling principles per classification level are presented in Figure 8. (Kansallinen turvallisuusviranomainen 2020, 2,5,30)



Classifications in 2010–2019	Classification as of 2020
ERITTÄIN SALAINEN, protection level I (ST I)	ERITTÄIN SALAINEN TL I
SALAINEN, protection level II (ST II)	SALAINEN TL II
LUOTTAMUKSELLINEN, protection level III (ST III)	LUOTTAMUKSELLINEN TL III
KÄYTTÖ RAJOITETTU, Protection level III (ST III), Protection level IV (ST IV)	KÄYTTÖ RAJOITETTU TL IV
SALASSA PIDETTÄVÄ, Protection level III (ST III), Protection level IV (ST IV)	SALASSA PIDETTÄVÄ

Figure 7. Secrecy and security classification levels.



HANDLING AND STORAGE OF INTERNATIONAL CLASSIFIED INFORMATION

Security classification level	Handling		
	Turvallisuusalueiden ulkopuolella	Hallinnollinen alue	Turva-alue
II SECRET	Paper documents: Yes, temporarily when additional demands are fulfilled* In terminal device: Yes, in a terminal device fulfilling the requirements and additional demands*	Paper documents: Yes, in case the unauthorised access is prevented In terminal device: Yes, in a terminal device fulfilling the requirements in case the unauthorised access is prevented	Paper documents: Yes, in case the unauthorised access is prevented In terminal device: Yes, in a terminal device fulfilling the requirements in case the unauthorised access is prevented
III CONFIDENTIAL	Paper documents: Yes, temporarily when additional demands are fulfilled* In terminal device: Yes, in a terminal device fulfilling the requirements and additional demands*	Paper documents: Yes, in case the unauthorised access is prevented In terminal device: Yes, in a terminal device fulfilling the requirements in case the unauthorised access is prevented	Paper documents: Yes, in case the unauthorised access is prevented In terminal device: Yes, in a terminal device fulfilling the requirements in case the unauthorised access is prevented
IV RESTRICTED	Paper documents: Yes, temporarily when additional demands are fulfilled* In terminal device: Yes, in a terminal device fulfilling the requirements and additional demands**	Paper documents: Yes, in case the unauthorised access is prevented In terminal device: Yes, in a terminal device fulfilling the requirements in case the unauthorised access is prevented	Paper documents: Yes, in case the unauthorised access is prevented In terminal device: Yes, in a terminal device fulfilling the requirements in case the unauthorised access is prevented

Figure 8. Principles for the processing of classified information.

Network infrastructure management

Control I-04 takes a position on how administrators should implement management connections in a security-based manner to interfaces of different systems, such as firewalls, routers, switches, wireless access points, servers and workstations. The control warns that classified information can be accessed directly or indirectly through different management tasks. The database administrator has direct access to the data in the database, but the network equipment operator can indirectly influence the operation of the database, e.g. by the database firewall settings. This type of case could be of particular interest to the hostile actor. For example, the control aims to highlight and demonstrate that if a direct and indirect management link has access to classified information, the device used for management and the connections should be operated in the same security class as the managed data processing environment. (Kansallinen turvallisuusviranomainen 2020, 72)

In exceptional cases, lower-level environmental management from a higher-level management environment may be performed, but there is a requirement that the gateway solution approved by the Authority should be used at the limits of the safety classes to prevent the transfer of information of the upper classification level of the data to the lower-level environment. (Katakri, 2020, 72)

Control I-08 requires compliance with the principle of minimum functionality and least privileges i.e. in practice system hardening is carried out through controls on network devices, server, workstations, mobile devices and printers. The new systems come with a lot of features and not all features may be necessary for the use of the core of the system. In many cases, devices have unnecessary settings turned on that open up opportunities for the hostile actor to take advantage of weaknesses of services. For instance, systems can have default user accounts with a default password. The aim of hardening is to minimise system settings in order to reduce their vulnerability area. The aim is therefore to have the necessary settings configured for use in the systems. (Katakri, 2020, 80)

Hardening also includes item management connections, which should be limited, user-identified, hardened, and session time-limited. In principle, the requirement for the systems is to be hardened according to manufactures’ hardening recommendations or general hardening instructions should be used. Hardening can also be approached based on risk assessments. (Katakri, 2020, 80)

Remote management

The control I-18 emphasises that the protection of management connections is one of the most important and critical points that affects the security of information systems. Control requires for sufficient reliance on the identity of users and equipment and provides guidance that classified information shall be protected from bystanders if handled outside the security areas. Staff should be trained in secure remote management. The criteria require remote access to be carried out only for the processing of level IV classified information. ST III confidential level material is processed in accordance with a physically protected space approved by the authority or in exceptional circumstances, other compensating methods of protection are applied. (Valtiohallinnon tietoturvallisuuden johtoryhmä, 2012, 51)

Segmentation

The isolation of networks of information systems into different segments can significantly contribute to the protection of classified information. As regards the segmentation, the criteria aim to achieve a safe environment for the processing of classified information at different levels and to isolate different safety class processing environments. It is not possible to process upper-level data in a lower-level handling environment but vice versa it is possible, and the processing can then be carried out in such a way as to comply with the protections specified for the higher classification level. I-01 control requires at least the use of a firewall solution between environments of different levels of safety class. Secondly, class III-II requires gateway use approved by the authority if the data processing environment is combined with that of other safety classes. (Katakri, 2020, 65)

The control emphasises that if a safety class crossing occurs in the case of management traffic, a gateway solution for the operation of the management approved by the authority is required. (Katakri, 2020, 65)

A data network can have different roles, ranges or functions that are targeted different strengths of security level requirements. Segmentation can be carried out by dividing the networks into separate subnets and logical virtual networks by implementing it through firewall functionalities. Virtual networks are typically used in these activities:

- **Production network** or **office network** in which the standard user and workstations are involved.
- **A maintenance network** through which network systems and network devices are managed. The user must be strongly identified when logging in to management services. The network infrastructure can be implemented in such a way that the maintenance network is completely separate from the production network, in which case network equipment management is not prevented in the event of a malfunction in the production network
- **Server network**
- **A test network** that tests equipment, programs, and configurations separately from the production environment.
- **A DMZ** network where services are placed for users outside the internal network, such as www, external DNS and gateways to the internal network.
- **Guest network** with the lowest security level. Intended for occasional use by visitors. (Valtiohallinnon tietoturvallisuuden johtoryhmä, 2010, 24)

Logging and monitoring

The I-10 control prompts the following devices on workstations, servers, network devices such as firewall, and also workstation's firewall are collecting logs. The log data is collected for anomalies, and it can be used to prove which activities have been carried out on the environmental assets and who is behind the action. The control mentions that an event's log of the network administrative tasks should be available, indicating what actions have been taken in the network, what has been the purpose of the operation and who is behind the action. The recommended method is to redirect key log data to a centralized and robustly secured log server, whose data should be backed up daily in an environment at least of the corresponding security class. (Katakri, 2020, 85)

2.1.4 PITUKRI

Pitukri contains interpretations and guidelines for assessing the risks associated with cloud services. In addition, it brings together good practices affecting the security of cloud services that can also be used both in commercial operators and the private commercial sector operators to protect business-critical services and information. The criteria help in the acquisition of new cloud services and in the assessment of the security of existing cloud services. (Traficom 2019.)

Network infrastructure management

IP-03 is an encompassing control that incorporates many aspects of the same requirement, such as system management methods, segmentation and management connection protection requirements. For access to management, strong authentication is required for user identification, for example password and token-based combination with at least two authentication factors. The control has instructed that, in principle, less secure environments and terminal equipment cannot be managed in an environment intended for the processing of classified information. (Traficom, 2020, 37)

Remote management

The cloud environment is typically managed remotely because maintenance takes place from outside the data center environment. The requirement is that management is performed through limited, managed and controlled points, such as jump hosts, admin portals and similar portals. Access to management requires a strong user ID based on at least two authentication factors. Management is advised to use the appropriate encrypted method to guarantee integrity. (Traficom, 2020, 37)

Segmentation

The first paragraph of IP-03 requires that management access is performed in a cloud environment through jump hosts, management portals or the like placed at its own limited and controlled points. If there are several control points e.g. in the case of a cloud services provider, they need to be differentiated so that the services to be achieved remain clearly separate from each other. (Traficom, 2020, 37)

Logging and monitoring

JT-01 control requires for event logs to be collected for deviations from system operation, user activities, security-related events and exceptions. It is recommended to collect logs as widely as possible from different systems and equipment such as workstations, servers, network equipment, especially from host firewall and boundary firewalls. It is best practice to redirect all logs to a centralized server and it is also necessary to ensure that collected logs are strongly protected and backed up regularly. The content of the log data must be sufficiently comprehensive to verify the data breaches and their attempts afterwards. According to the control, logs should be transmitted from log sources to the log collector in a secure manner so that the parties are truly identified. Alternatively, log data can be transmitted over the management network to SIEM. Network equipment and other network asset clocks need to be synchronized with a centralized time service. When the number of logs is high, there is a need to obtain automation. Separate alarm tools for the observation of deviations in network traffic can be improved by placing sensors in key network nodes, as well as in workstations and server which can also provide indications of abnormal operation. This requires knowledge of the normal state of network traffic. For better traceability, the jump host policy can be used, where all maintenance operations are carried out and efficient logging is carried out through the jump host. (Traficom, 2020, 38)

2.1.5 ISO27001

ISO 27001 is part of growing ISO/IEC standard family that defines requirements to establish, implement and maintain organization's information security management system, and to constantly is improve it. ISO27001 main cornerstone is to protect the confidentiality, integrity and availability of the information. The standard guides risk-based thinking that maps safeguarding the assets and determines their level of criticality. The risk management plan is built on the risks that are identified and assessed. (Itewiki, n.d.)

Remote management

Remote work is usually carried out at home, but it allows people work on a train, at café, at meetings or elsewhere outside the workplace, and different methods of connecting to the organization's internal services are used. There are more risks associated to remote work than working at office. The risks include for example physical safety, as workplace equipment can be available to other people such as family members and visitors. It is important for a teleworker to be aware of the risks involved in remote work and to know what kind of practices should be taken. Remote work policy and operating models must be defined by organization. Partly through defined practices and processes, it is possible to reduce the risks. (Kenyon, 2019, Chapter 2)

In an operating environment, it should be ensured that the information processed cannot be destroyed, damaged, compromised or modified. The organization and the connections between the functions should be protected. Remotely accessed data should be limited to a minimum. (Kenyon, 2019, Chapter 2)

Segmentation

It is difficult to secure large and complex domain environments, hence they may be divided into numerous separate local network domains. Each domain has its own function, such as desktop access, finance and marketing. Different trust levels are represented in the domains. Firewall can be used to control access and data flow between the local networks. Traffic can be limited by a firewall based on a risk assessment. Risk assessment should be performed on each domain separately in order to block the prohibited access. (Calder & Watkins, 2020, Chapter 19)

Networks of companies are often exposed and vulnerable to unauthorized access that may pose a risk to network operations and related components. The situation may lead to a shattering of reliability and the disintegration of integrity for the network or its components. IT infrastructure faces more risks the larger it is and therefore securing of large networks can be challenging. Dividing the network into physical and look domains can make the security management easier.

Each network zone should be viewed separately within the organization. Risk assessment is carried out for each of them to determine the level of security. Robust segregation of networks is achieved by implementing routing and network connection controls. (Kenyon, 2019, Chapter 2)

Logging and monitoring

In control A.12.4.3, the requirement is to log the actions of administrators and system operators. Logs should be protected and checked regularly. The following identifiers should be included in the log data:

- System or event starting and finishing times
- Persons involved
- Event information (event)
- System errors (what, date, time) and corrective actions taken

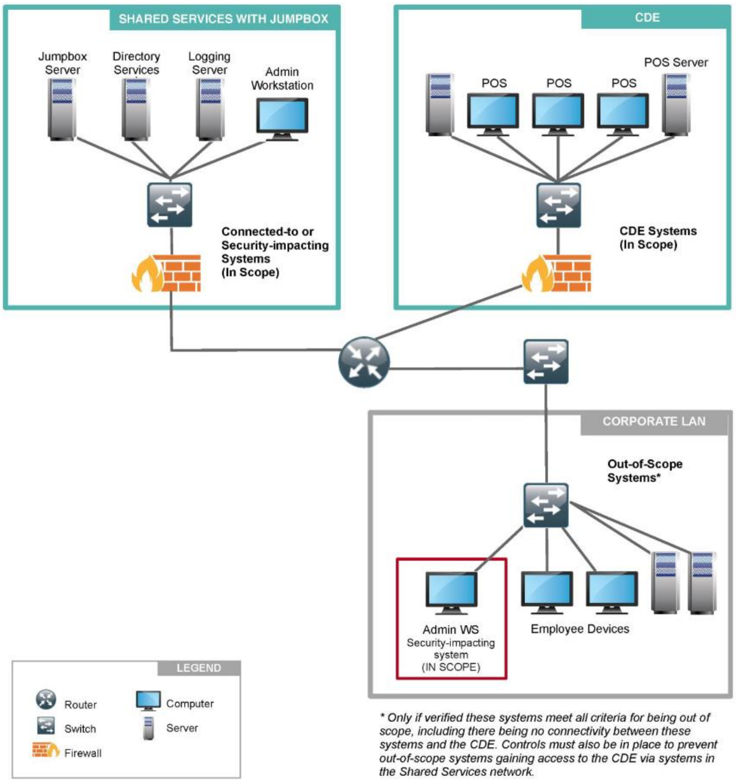
Network admins and systems network management activities can be monitored using the intrusion detection system (IDS). Since administrator’s activities are monitored, monitoring and IDS maintenance, as well as control, should not be administrator’s responsibility, to preserve the integrity of log data from someone other than the admins. The following matters should be involved in the logs: the time when an event occurred, relevant and useful information about the event is provided. (Calder & Watkins, 2020, Chapter 2)

2.1.6 PCI DSS

The Payment Card Industry Data Security Standard contains requirements to ensure that company’s all processes, storing or transmitting credit card information is maintained in a secure environment. The purpose of the criteria is to improve the security of the consumer card payments worldwide, and the aim is to get companies to process card data in a consistent manner. (Groot, 2021)

Network infrastructure management

The Figure 9 (PCI Security Standards Council, 2016, 21) shows one example of how to implement a control. Administration can only be performed through a jump server. The criteria define precisely that connections must be prevented from other environments to the cardholder data environment (CDE), only those systems that have access to the in scope or for other specific reasons, are accepted. Normally, corporate LAN environments are not allowed to connect to the CDE environment or in the other direction. However, in the Figure 9 the admin’s workstation is placed in the corporate LAN network, which meets the requirements and is defined in scope. (PCI Security Standards Council, 2016, 18-21)



** Only if verified these systems meet all criteria for being out of scope, including there being no connectivity between these systems and the CDE. Controls must also be in place to prevent out-of-scope systems gaining access to the CDE via systems in the Shared Services network.*

Figure 9. PCI DSS model of the network infrastructure management.

Performing of admin management is described in generally the Figure 9. The figure shows that admin management can only be performed from an admin workstation of a LAN network and the management is established by connecting to the jump server and allowing connections to the CDE environment. (PCI Security Standards Council, 2016, 18-21)

Remote management

Control 8.3 requires MFA use to secure all non-console administrative access and all remote access to the CDE. Non-console administrative access refers to, as logical access to control is done by network route. In that case, no direct or physical connection to the system interface will be established. In practice, different type of the connection is performed from within internal networks or from external establishing non-console administrative accesses. The requirements advice to use at least two out of three authentication methods for the authentication. Control 8.3.2 separately requires MFA access to the remote network in general for all users, it is also required of third parties and administrators. (RSI Security, 2018)

Segmentation

Main point of the criteria regarding segmentation is to keep in-scope systems and out-of-scope systems separated from each other. Practically, this means that communications are prevented from out-of-scope systems to CDE environment that is called as in-scope environment. The out-of-scope system does not have access to the CDE meaning that the connections from an untrusted network are not allowed to access the CDE. In turn, in-scope systems have a direct connection to cardholder data. (Glover, 2017)

The CDE and out-of-scope systems are properly kept separate by using different technologies and process controllers. As a result of proper segmentation, no out-of-scope environmental components can compromise the safety of the CDE environment. Even if the hostile actor tries to establish a management connection from the out-of-scope system it would be prevented. (PCI Security Standards Council, 2016, 6)

Segmentation in methods is usually applied by using firewall and router settings to prevent traffic from untrusted networks to enter the CDE network. Physical access controls and network configurations to limit connections between different systems and subnets. (PCI Security Standards Council, 2016, 6)

In the PCI DSS criteria, several models of how the segmentation could be implemented are presented in the Figure 9. There are several ways of implementing segmentation for the network that works expectedly in one network and the other network does not achieve the benefits that are pursued. However, to provide efficient segmentation for the network, each segmentation method must be piloted against PCI DSS requirements to ensure that it works in line with the objectives. In Figure 9, the example describes three different network segments: shared services, CDE and Corporate LAN networks. (PCI Security Standards Council, 2016, 15)

The requirements of the criteria determine where management may be carried out and where CDE cannot be obtained for the environment. The purpose of the example is to bring in a single solution that can be used to implement segmentation where a CDE network is effectively blocked from the corporate network to which direct management connections are blocked. However, shared services on the network could support both networks. (PCI Security Standards Council, 2016, 15)

Logging and monitoring

Control 10.2.2 takes into account all credentials with elevated privileges, such as the root, admin or administrator that have full control of a network and access to all sensitive information that can significantly compromise the security or organization’s system. Without logging administrator actions, it may lead to a situation where problems appear in administrator error and shortcuts are used by giving privileges rights for a specific purpose when situations may not be monitored. (Baykara 2020)

There are at least three points of logging and monitoring to which particular attention should be taken in PCI DSS. The first one emphasises situational awareness aiming at obtaining the fullest possible clarity on the status quo. It should be considered what is happening on the server at certain moment and by whom the control is performed on the server, It needs to be observed who has gained access to the organization’s network or what a certain application does with the card data. The importance of logging and monitoring is emphasised when there is a need for information and realisation material or incidents breach. That information also improves the later incident response. Secondly, it takes IDS to detect threats to get information about the nature of the threat. Thirdly, logging is the guiding factor in network infrastructure and security management, providing valuable information on how and where security controls should primarily be targeted at blocking and blocking measures. One example is to use firewall logs to detect intrusion. (Branden & Chuvakin, 2015, Chapter 10)

2.1.7 Collected security controls from frameworks

Security controls related to IT administration and functions are aggregated in a single spreadsheet. The table has a total of 67 controls that can be used to improve information security if an existing control or its own controls cannot mitigate the risk. This serves as an additional tool for the organization when considering new controls against threats.

2.2 Risk analysis

Risk analysis is one part of the risk assessment. Based on the risk analysis, actions to measure, and management and mitigation methods to threats can be determined. Harmful events can be managed through operation culture, process and structures. The risk analysis provides a cross-section and information on the most critical risks to the organization's operations. The nature and the severity of the risks are assessed as well as their probabilities and impact on the organization's activities. The risks are determined by measures to mitigate them and to take control of the risks to enable normal operation for the core of the organization. The most critical risks are brought to the attention of the key personnel of the organization, in order to situational awareness can be maintained, and lager lines can be agreed together to manage the risk. Some of the risks may not be eliminated. Decisions how to take control of the risk or whether to take a conscious risk with regard to some threats should be made by stakeholders and key personnel.

Risk analysis is one part of the risk assessment. The purpose of the risk analysis is to understand the elements related to the risk and more deeply what the risk holds. The aim is to find out the nature, quality and level of risk. When a risk analysis is performed, different perspectives are considered e.g. source of the risks, reaction, probability, events, scenario and impact. (Finnish Standards Association SFS, 2018, 35)

The risk consists of cyber threats, vulnerabilities and incidents that can cause damage to organization's assets, i.e. information systems and various functions. The risk level can be determined through an impact assessment that is calculated using the following formula: impact * likelihood = risk (I*L=R). The level and severity of the risk to a particular asset is assessed from the point of view how high the probability that the threat will materialise and how much impact it would have on the identified asset. In order to establish the level of risks, it is necessary to carry out an in-depth analysis of threats and vulnerabilities. Analysis helps to understand which factors are related to the risks. This contributes to providing directions for what measures can be taken against risks. (Stølen et al., 2015, Chapter 2)

The risk analysis is performed representatively when the information security audit of a system or the planning phase is performed. In the information security audit, one of the most important tasks is to assess the capability and effectiveness of the control mechanisms applicable to the information technology items and generally, the architecture of the information systems. During the audit, the effectiveness of the information processing system is evaluated, and the security of the technologies used is assessed. When considering solutions, securing of the confidentiality, integrity and availability of an organization's assets should always be kept in mind. (Kuzminykh et al., 2021)

In the risk analysis phase, each identified risk is assessed and adequately described. Practically, during risk analysis it is assessed which threats are targeted at each safeguard IT asset. In addition, it can be assessed how largely the same threat affects different assets and which routes or rather what vulnerability is exploited a threat can take to reach the target. The risk analysis focuses on those risks that pose internal and external threats to the confidentiality, integrity and availability of the organization's data. (Brooks 2020)

The phases of the risk management process are definition of the operation, evaluation of the process and treatment of the identified risks. Each phase involves monitoring, review, communication and exchange of information. The risk management process is presented in Figure 10 (Finnish Standards Association SFS, 2018, 32).

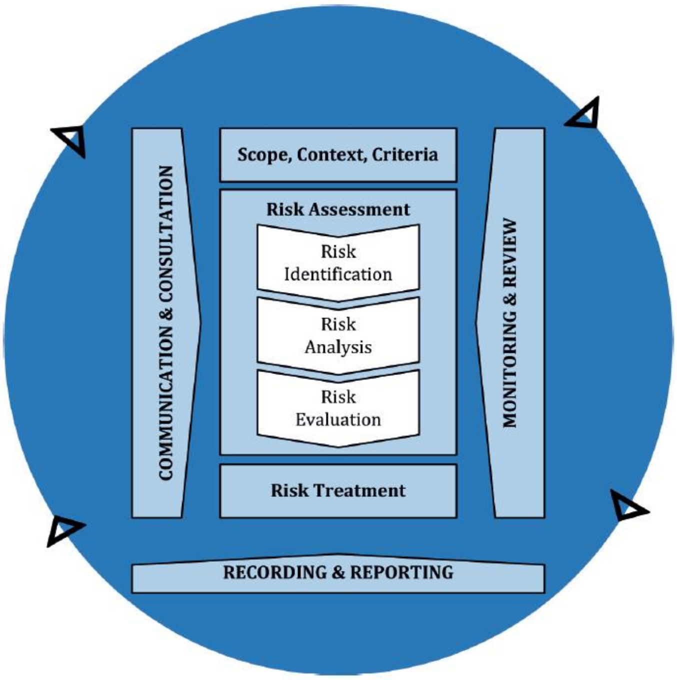


Figure 10. The risk management process.

2.2.1 Qualitative and quantitative risk analysis

The security risk analysis can be performed by using three methods, qualitative or quantitative analysis or a combination of them. A qualitative analysis technique is subjective and the most commonly used method because of a clearer and easier way of highlighting the most relevant findings about the severity of critical risks. The results of the analysis may be presented in a form of risk matrix that provides the most up-to-date information to stakeholders. The risk analysis is usually performed using three risk levels (low, medium, high), but each organisation decides for itself which criteria to use for classification. A quantitative analysis technique is more objective and deals with numbers. (Kuzminykh et al., 2021)

Semi-quantitative analysis method may be used as an intermediate form of quantitative and qualitative assessment method. This method uses a qualitative method as an aid to determine the level of risk by using a formula. The semi-quantitative method differs from the qualitative method by using numerical assessment scales to assess the consequences and probabilities. (SFS-EN 31010, 2019, 145)

2.2.2 Asset management

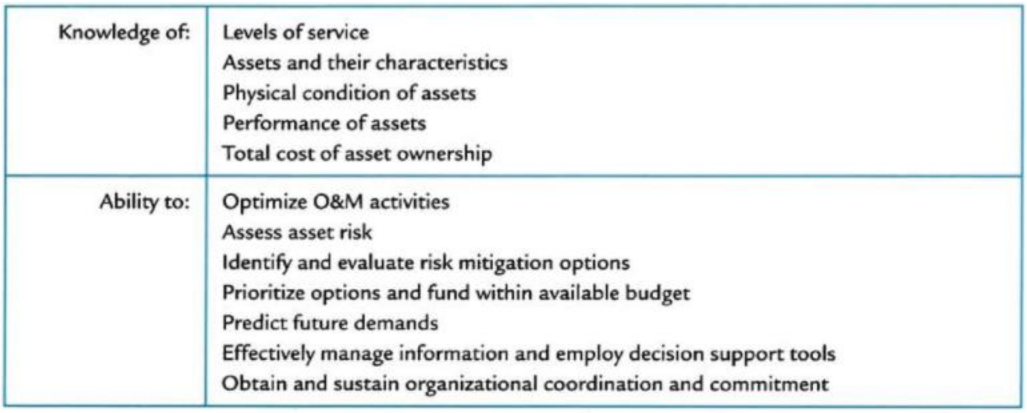
Asset management is a significant part of successful business, because the company’s assets are the factors that generate value for the business. Asset management aims to understand the value of the assets owned by the organisation. (Souza et al., 2022, 214) The core idea of asset management can be defined in this way:

> *“An integrated set of processes to minimize the life-cycle costs of infrastructure assets, at an acceptable level of risk, while continuously delivering established levels of service”* (CH2M, 2007, 9)

Asset management could be thought as a set of processes instead of a single process and it is not an individual project or task, but business practice that must be performed repeatedly. These types of processes belong to asset management:

- Asset identification
- Classification
- Valuation
- Impact assessment (SFS-ISO /IEC 27005, 2018)

For efficient asset management, risks are balanced between minimizing costs and achieving desired services levels. It assists the upper layer managers to understand and define the risks damaged or breached assets and risks are managed those risks will not rise above acceptable levels. Effective asset management includes the following key concepts as shown in Figure . (CH2M, 2007, 9)



Knowledge of:	Levels of service Assets and their characteristics Physical condition of assets Performance of assets Total cost of asset ownership
Ability to:	Optimize O&M activities Assess asset risk Identify and evaluate risk mitigation options Prioritize options and fund within available budget Predict future demands Effectively manage information and employ decision support tools Obtain and sustain organizational coordination and commitment

Figure 12. Key Concepts for Effective Asset Management.

2.2.3 Scenario method

Scenario analysis is one of the techniques that can used as a tool for risk assessments. The core point and the benefit of scenario analysis is to understand risk and opportunity. Through scenarios, unpredictable outputs may revealed and which encourages creative and a free exchange of ideas. This method encourages people to think widely different kind of potential outputs. (U.S. Department of Homeland security 2018, 9)

In scenario-type analysis different cases/ways to identify potential threats are examined. At the beginning of the analysis a scenario is created. Previous security breaches and near misses worth taking advanced should be considered when the scenario is composed. General data security related material can be used as guidance. Based on analysis, security IT state and potential security flaws are pointed out and cases are drawn up. In order to achieve the the most complete scenarios, it is advisable to bring in specialists and staff from different departments in different areas of expertise. (Valtiohallinnon tietoturvallisuuden johtoryhmä, 2003, 88)

3 Implementation

3.1 Current state analysis

At the beginning of the work, a query was arranged for the personnel to pose a current state of IT management. The query was used to orienteer and prepare for future workshops where risk analyses were performed on the basis of observations. The query included 24 multiple-choice questions and open-ended questions (Appendix 1). A few questions have been removed because of sensitive information. A question matrix was in connection to several questions to find out how often a specific method is used. The frequency options were: once a month or less, once a week, several times a week, daily and several times a day.

In more detail, the query aimed to identify which tools and working methods each employee uses and how often. The query also sought to understand how uniform management methods are among employees. Each employee has a certain responsibility in the team, but the same type of tasks are performed in daily maintenance work. This will determine where the management is focused among users. The query also aimed to identify problem areas and security challenges that occur in the performance of work tasks.

Efforts were made to position the questions in such a way that several options were added to the multiple-choice questions to make it easy to aggregate answers for analysis. Efforts were made to minimise the number of open-ended questions, but the respondent was also given the opportunity to answer questions freely so that the comment box was embedded as an option in the multiple-choice question field.

The query mapped which methods and tools are used to manage IT from different locations and what kind of practices are included in the maintenance work. Replies to the anonymously organised questionnaire were received from seven IT employees. Respondents were experts in support, SQL, workstation and server environment.

3.2 Workshop

During the thesis, workshops with IT employees was arranged remotely. In the workshops, protectable assets were mapped. As many threats to IT administration and its assets as possible were identified. The nature and reason for the threats and the consequences that threats would cause when realised was described and documented. In addition, risk analysis was performed on threats and their likelihood and impacts were discussed and assessed.

The workshop had three main stages. In the first stage, the results of the query and the observations made by the thesis author were reviewed and how to the pass-the-hash attack was carried out. Risk assessment methodologies were also presented, classification of threats in scales and measures definition tables. In the second stage, people were divided into two groups of three participants and the groups identified protectable assets and possible threats using a pre-made threat map as an aid (Appendix 2). The threats were classified in accordance with People, Process and Product principle. In the third stage, the risks were addressed, and the probabilities and impacts of the risks were assessed and measures were considered to reduce or remove the risk completely. The workshop used the following documents and tools:

- Teams for organising the workshop
- Pre-made threat map for supportive use
- Miro Whiteboard platform for identifying assets to be protected and the threats (Appendix 3)
- Risk analysis -excel
    - Threats classification file
    - Definition of measures file

3.2.1 Risk matrix

A 4x4 level semi quantitative risk matrix was used in the risk assessment. The values of the risk matrix were determined according to the likelihood and impact criteria in the classification of threats. The probability and impact values for the risk assessment were determined according to the risk matrix presented in Table 1.

Table 1. A 4x4 semi quantitative risk matrix.

Likelihood	4	🟨	🟧	🟥	🟥
	3	🟩	🟨	🟧	🟥
	2	🟩	🟨	🟨	🟧
	1	🟩	🟩	🟩	🟨
		1	2	3	4
		Impact			

🟥	Intolerable risk
🟧	Significant risk
🟨	Notable risk
🟩	No risk

3.2.2 Risk categorising

The assessment of the magnitude of the risk shall was performed based on the likelihood and impact assessments. In this work, the threats were classified as shown in Appendix 4.

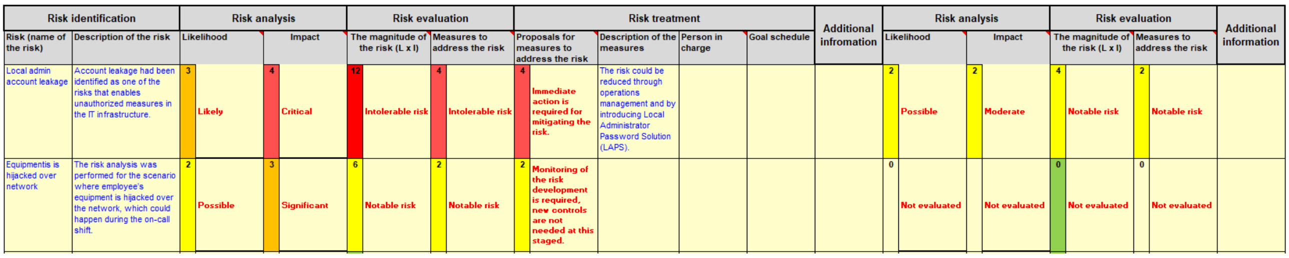
Once a certain threat was assessed for its risk value, the risk value was mirrored against the risk categories and corresponding actions needed to deal with the threat in the future. The risk categories and the actions are presented in Appendix 5.

After the risk assessment, controls were selected for the target to be protected to reduce the risk. The risk analysis was re-performed to show how much the control had reduced the risk. The results of the risk analysis can be compared between current and after control effect, which also determined the residual risk.

4 Results

4.1 Risk analysis stages

Risk management tool was used in the workshops to carry out the risk analysis including all stages of the risk assessment such as risk identification, risk analysis, risk evaluation and risk treatment, as shown in Figure 13. In addition, a new set of risk assessments was set up as an extension of the main table for the sections to be used if a risk was classified as a significant or unacceptable. In these cases, the risk assessment was re-performed to see how well the defined controls could reduce the risk and to get result of the residual risk. The goal was to find and determine proper measures and robust controls to mitigate and reduce the risk so well that the risk fell on the green area in the matrix. The green area indicates that there is no risk and no need for further controls are needed. The assessment of the risks and assets and their consequences resulted in a numeral assessment and determination of the severity and magnitude of the risk. This numeral assessment guided the selection of further actions in accordance with the risk categories.



Risk identification		Risk analysis		Risk evaluation		Risk treatment				Additional infromation	Risk analysis		Risk evaluation		Additional information
Risk (name of the risk)	Description of the risk	Likelihood	Impact	The magnitude of the risk (L x I)	Measures to address the risk	Proposals for measures to address the risk	Description of the measures	Person in charge	Goal schedule		Likelihood	Impact	The magnitude of the risk (L x I)	Measures to address the risk	
Local admin account leakage	Account leakage had been identified as one of the risks that enables unauthorized measures in the IT infrastructure.	3 Likely	4 Critical	12 Intolerable risk	4 Intolerable risk	4 Immediate action is required for mitigating the risk.	The risk could be reduced through operations management and by introducing Local Administrator Password Solution (LAPS).				2 Possible	2 Moderate	4 Notable risk	2 Notable risk	
Equipmentis is hijacked over network	The risk analysis was performed for the scenario where employee's equipment is hijacked over the network, which could happen during the on-call shift.	2 Possible	3 Significant	6 Notable risk	2 Notable risk	2 Monitoring of the risk development is required, new controls are not needed at this staged.					0 Not evaluated	Not evaluated	0 Not evaluated	0 Not evaluated	

Figure 13. Risk management tool.

The risk analysis was started with assigning a risk, that had been identified during the asset and threat mapping. After this, the nature of the risk was described in the table and what the risk is related to and what could be happen if the risk would realise.

After the risk description, the likelihood and impact of the risk was assessed with the participants using a threat classification that showed the criteria (Appendix 4) for likelihood and impact assessments. Once the likelihood and impact of the risk had been added into the table, the final result on the magnitude of the risk was obtained. This result guided how to the risk would be addressed in the future. Appropriate controls and tasks were assigned to remove or mitigate the risk. The organization might have own controls to mitigate the risks but if not, the controls were obtained from collected controls from well-known criteria. The end of the risk assessment, the executor of controls and the person in charge of the project was assigned with schedules.

4.2 Overall results of the risk analysis

Unfortunately, all risks could not be published in this thesis because of their sensitivity, hence most of all medium and high-level risks had to be excluded and the risks were purposed solely for the organization's knowledge. However, two risks were considered more detailed in this part and all stages how the risk was handled during the workshop was described.

Table 2 shows the statistics of overall results of the evaluations and mappings. During the workshops, protectable assets and threats were identified and separately, the asset-by-asset assessment of the threats to them. Based on asset and threat mapping 9 significant risks raised and were taken into consideration for risk assessment. By mitigating the risk, there were plans to use numerous controls which have been selected from collected criteria.

Table 2. The statistics of overall results of the evaluation and mappings

Evaluation	Quantity
Assets	50
Identified threats	62
Threat mapping for the assets	18
Risk analyses	9
Controls from collected criteria	18

Table 3 shows the statistics of the results of the risk assessment. It presents how many risks were identified and how many measures were done to mitigate the risks and how many risks were monitored.

Table 3. The statistics of the results of the risk assessment

Risk level	Identified risks	Measures	Risk monitoring
No risk	0	Not required	-
Notable risk	3	Not required	3
Significant risk	2	2	2
Intolerable risk	4	4	4

4.2.1 More detailed results of the risks

A few identified risks with more detailed information are presented below. Part of the risks could not be presented due to the confidentiality of the information. As shown earlier, the Figure 13 shows two risks of different severity that were identified during the workshop. One of the risks is classified as highly critical, requiring immediate action and the other one is less severe in which the outcome of the assessment monitors the development of the risk.

The first identified risk was local administration account leakage. This had been identified as a risk that enables unauthorized measures in the IT infrastructure. This can occur when a machine has been compromised through a vulnerability that allows an attacker to steal account from the computer and possibly use it to bypass security controls. In addition, the attacker can possibly move laterally in the network from one computer to another and the attacker could obtain critical assets, sensitive business data or administrator credentials. This type of risk was assessed as likely to materialise and the severity of the risk was classified to a critical level, in which case the overall result of the risk indicated that there was an unacceptable level of risk. The likelihood was assessed to be at level *notable risk* and the value of the impact was at level *critical risk*. The overall of the risk was evaluated as *an intolerable risk*. In this case, the risk is severe and immediate measures and controls were needed to eliminate or reduce the risk. A number of measures have been assigned, such as the deployment of Local Administrator Password Solution (LAPS) and the complete deletion of the account has been considered.

As a control the organization decided to deploy the Local Administrator Password Solution (LAPS) with additional hardenings as a countermeasure to local administrator leakage. These mitigations can significantly restrict the ability of attackers to use administrator's local accounts for lateral movement Pass the Hash (PtH) attacks. The measure was the correct solution and well-founded for this situation because local administrator's accounts are only available to administrators and grants are not authorized for standard users and developers. In complex environments, other solutions may have to be considered.

The risk analysis was re-performed after deployment of the LAPS and other additional hardenings to get the result of the residual risk and also to get indications of how well the controls work. The residual risk was assessed in the risk analysis for the risks that had been classified as *notable risk* as shown in the

Figure 13. Risk management tool.

. The likelihood was assessed to be at level *possible* and the value of the impact was at level *moderate*. The overall of the risk was evaluated as a *notable risk*. The risk was reduced from intolerable risk to notable risk and the overall risk level reached an acceptable level. The risk has been significantly mitigated; hence, further action was required to monitor the risk development. New controls were not needed at this stage.

Second risk was detected for the scenario where employee's equipment is hijacked over the network and it allows to feed malware to the equipment. This could happen for example at shopping center or cafeteria during the on-call shift. In the workshop, it was assessed the scenario could be *possible* and its effects could be *significant*. As a result of the assessment, monitoring of the risk development was required and therefore new controls were not needed at this stage. However, the table contains proposals for measures if the risk would increase.

5 Conclusion

The goal of this work was to find out the methods that can improve the organisation's information security. In addition, those risks that compromise IT maintenance operation were identified and areas of development were mapped to improve security.

The result of the research and the risk management model developed during this work are particularly useful for those organisations and IT administrations that have not yet invested in improving risk based information security. In this work, tools and clear phases were created to highlight the risk and development targets with a reasonably light model. The study also provided concrete examples of risks and corrective measures, as well as controls to mitigate risks.

The study made extensive use of several security criteria, which have not been utilised as comprehensively in other studies in the IT maintenance area. This work gives visibility to how well the different criteria have controls to secure IT maintenance work. The work showed that it is worth using several different criteria, as the controls related to maintenance work might not be sufficiently comprehensive in a singular criterion. In addition, it was noteworthy that for example the PCI DSS criterion is provided for companies working in payment transport, but the criteria contained a lot of useful controls for the maintenance and other sectors. Hence, the use of PCI DSS criterion can be highly recommended also for other industry areas.

The risk management method developed for the organisation was found to be suitable for risk management. The risk assessment stages were clear and the criteria for risk assessment were appropriate. Efforts were made to obtain the most accurate and correct possible assessment of the risks collectively, which provided a stronger and more convincing outcome on the basis of which measures and mitigating methods can be determined to eliminate and minimise the risk. The author suggests that the risk assessment alone should not be considered sufficient.

Risk analysis and assessment processes were proceeded in moderation, e.g. it may have taken a lot of time to describe the risk and assess its severity, but that is understandable because the assessment must take into account so many factors that affect the outcome of the assessment. However, in risk analysis, it is important to focus on a deeper understanding of risk and what the risks may cause to the organisation’s operations if it realised.

The risk management tool serves as an adequate tool for monitoring. Risk management is a continuous activity. The tool is a good indicator of how the situation has been improved after measures taken and the tool serves as a good indicator for assessing whether the severity of the risk is at an acceptable level or not.

5.1 Research questions

Are there any ready-made controls in the existing security frameworks?

The work dealt very extensively with the controls of different criteria that hit the IT maintenance sector. Mapping of controls was facilitated by dividing them into various topics such as IT administrative operating models, network infrastructure management, identity management, access management, remote management, segmentation and logging/monitoring. The coverage of the controls was perceived through the topics discussed. It is clear that more controls were found in certain criteria i.e. the broader the criteria, the more controls related to maintenance work were found. For instance, the NIST criteria are so wide that most of the controls were found there. However, there were surprisingly few controls in relation to the total number. A total of 67 controls from different criteria were listed during the research. Obviously, it can be stated that more controls should be found. It is obvious that these controls also belong to the IT maintenance sector, which improves the non-privileged employee’s field of activity. This work focused solely on enhancing information security related to IT maintenance work, which is the reason for the low number of controls.

Did significant risks detect during the risk analysis?

As indicated in section 4.2, significant risks were found during the workshops, which required immediate measures to eliminate or reduce the risk. During the work, a lot of threats that target different assets were identified, which ultimately poses a risk to the organization’s operations. However, the main focus of the work was on analysing and evaluating significant risks. There were a lot of risks on the list, but the most significant risks were selected for the assessment.

6 Discussion

The thesis changed shape during the project. At the beginning of the project, there was an idea that technical implementations would be included in the work. As the project progressed, it became clear that the technical implementation would not fit in the scope and schedule. In the work, it was decided to focus more on risk-based and systematic thinking. Firstly, we thoroughly identified the risks to the activities and analysed and evaluated them. Perhaps this focused more on finding the root causes of the risks and assessing their severity, which will make it possible to better justify the measures required and to justify to stakeholders why investments are needed to minimise the risks.

According to the representative of the host company, the workshops were necessary, and the results were valuable. The outputs of the observations and risk analyses received in the workshops will lead to several measures. In addition, the risk management method was found useful during the process and the method will be used in risk assessments also in future. The workshops were arranged remotely, but even more productive workshops could be arranged face to face.

6.1 Ethical Principles, quality and Data Protection

No personal data and copyright material are included in the text, research or other accompanying materials of the thesis. The research is organized anonymously, and the survey data has been properly stored during the thesis writing process. The query data is deleted when the thesis project is finished.

The study used reliable sources and research. The author respects the work and achievements of other researchers, referring to their publications and results in an appropriate manner. The quality of the research was ensured by the fact the materials needed for the research were collected mainly from scientific sources and well-known criteria. Above all, the aim was to find and utilize a lot of new research. The statistics were collected from well-known reports and information security research actors who have been studying the development of threat trends for years.

The confidential matters dealt with in the thesis have been kept safe with the various parties involved in the thesis and the obligation of confidentiality imposes it. In addition, at the beginning of the study, the signed agreement contains conditions for strengthening trust. With the representative of host company, it has been separately agreed on what matters, and observations can be made in the publication in the public part of the work. The results of the workshops have been discussed separately with the principal and agreed on how they can be presented in the work, but with aim of ensuring that the scientific community can also see concrete results. The author of the thesis respects the wishes of the principal and details of the organisation's environment are not published, which could cause harm and unauthorised behaviour towards them.

The author (Hertteli) has followed JAMK's ethical principles (JAMK university of Applied Sciences, 2018) and the *"Ethical recommendations for thesis writing at university of applied sciences"* produced by The Rectors' Conference of Finnish University of Applied Sciences. (The Rectors' Conference of Finnish Universities of Applied Sciences Arene 2019)

6.2 Development proposals

As mentioned at the beginning of the thesis, the technical implementation has been excluded from the work because it does not fit the scope. It would be adequate to continue the work on technical implementation and to consider a control whose need has been clearly come out as a result of a risk assessment. The technical implementation could be e.g. the introduction of a Privileged Access Workstation (PAW) principle or Privileged Access Management (PAM) solution. It is essential to keep the risk management tool as a guide in making decisions. It serves also as an adequate guide in how strongly the risk needs to be rectified. Before corrections, the likelihood and impact of the risk are assessed when a clear snapshot and an assessment of the magnitude of the risk are obtained. After assessing the risk, main focus should be kept on further work to improve the information security through technical implementation or by improving processes. An appropriate mitigating method or control is performed based on risk assessment. The mitigating method could be a control that significantly changes the operating models in the organization. After the change, a risk assessment is re-performed to determine the residual risk and real information on the functioning of the control is obtained. In addition to this, the same type of query that was done at the beginning of the work could be arranged for the personnel, which would also provide information on how the personnel have reacted to the changes in the operating models.

References

National Security Authority of Finland. 2020. Information Security Audit Tool for Authorities. *Accessed on 15 December 2021.* Retrieved from https://um.fi/documents/35732/0/FINAL+-+Katakri-2020_201218_en.pdf/705d2bc6-6f1b-90dd-52e1-1ef97dae0623?t=1625140100978

Verizon. 2021. 2021 Data Breach Investigations Report. Accessed on 15 January 2022. Retrieved from https://www.verizon.com/business/resources/reports/dbir/

Finnish Standards Association SFS. *2018. Risk management. Guidelines.*

BeyondTrust. 2021. Microsoft Vulnerabilities Report 2021. Accessed on 10 December 2021. Retrieved from https://assets.beyondtrust.com/assets/documents/BeyondTrust-Microsoft-Vulnerabilities-Report-2021.pdf

Calder, A., & Watkins, S. (2020). *IT governance: an international guide to data security and ISO 27001/ISO 27002* (Seventh edition). KoganPage.

CH2M HILL (Firm), N. A. of C. W. A. (U. S.), & Association of Metropolitan Water Agencies (U.S.), W. E. F. (2007). *Implementing asset management: a practical guide. Accessed on 9 December 2021.* Retrieved from http://app.knovel.com/hotlink/toc/id:kpINFNB0V6/implementing-asset-management

SANS Institute. 2021. *CIS Controls v8. Accessed on 8 December 2021.* Retrieved from https://www.sans.org/blog/cis-controls-v8/

Center for Internet Security. n.d. Telework and Small Office Network Security Guide. Accessed on 14 January 2022. Retrieved from https://www.cisecurity.org/insights/white-papers/cis-controls-telework-and-small-office-network-security-guide

Center for Internet Security. 2021. CIS Controls Version 8. Accessed on 10 December 2021. Retrieved from https://www.cisecurity.org/controls/cis-controls-list

Lukka, K. 2014. Kari Lukka: Konstruktiivinen tutkimusote. *METODIX. Accessed on 1 December 2021.* Retrieved from https://metodix.fi/2014/05/19/lukka-konstruktiivinen-tutkimusote/

PCI Security Standards Council. 2016. Guidance for PCI DSS Scoping and Network Segmentation. Accessed on 9 December 2021. Retrieved from https://www.pcisecuritystandards.org/documents/Guidance-PCI-DSS-Scoping-and-Segmentation_v1.pdf

Glover, G. 2017. How Does Network Segmentation Affect PCI Scope?. SecurityMetrics. *Accessed on 20 December 2021.* Retrieved from https://www.securitymetrics.com/blog/how-does-network-segmentation-affect-pci-scope

Australian Cyber Security Centre. 2012. Implementing Network Segmentation and Segregation | Cyber.gov.au. Accessed on 27 December 2021. Retrieved from https://www.cyber.gov.au/acsc/view-all-content/publications/implementing-network-segmentation-and-segregation

National Institute of Standards and Technology. 2020. *Security and Privacy Controls for Information Systems and Organizations* (Revision 5). *Accessed on 9 December 2021.* Retrieved from https://doi.org/10.6028/NIST.SP.800-53r5

U.S. Department of Homeland security. 2018. *SECURING HIGH VALUE ASSETS*. Accessed on 14 January 2022. Retrieved from https://www.cisa.gov/sites/default/files/publications/Securing%20High%20Value%20Assets_Version%201.1_July%202018_508c.pdf

Kenyon, B. (2019). *ISO 27001 Controls: A Guide to Implementing and Auditing*. *Accessed on 3 January 2022.* Retrieved from https://brad.idm.oclc.org/login?url=http://library.books24x7.com/library.asp?bookid=147715

Kuokkanen, A. 2020. *Newcomer's introduction to Privileged Access Management*. Accessed on 8 December 2021. Retrieved from https://www.theseus.fi/handle/10024/348503

Kuzminykh, I., Ghita, B., Sokolov, V., & Bakhshi, T. (2021). Information Security Risk Assessment. *Encyclopedia*, *1*(3), 602–617. *Accessed on 15 January 2022.* Retrieved from https://doi.org/10.3390/encyclopedia1030050

Leppänen, T. 2020. *Practical implementation of Windows end-point security controls*. Accessed on *10 December 2021.* Retrieved from https://www.theseus.fi/bitstream/handle/10024/139806/Leppanen_Tuomo.pdf?sequence=1

Lääkärikeskus Aava - Elämäntyönä terveytesi | Lääkärikeskus Aava. *Accessed on 3 February 2022.* Retrieved from https://www.aava.fi/yritys/laakarikeskus-aava

McGregor, C. (2018). Using Constructive Research to Structure the Path to Transdisciplinary Innovation and Its Application for Precision Public Health with Big Data Analytics. *Technology Innovation Management Review*, *8*(8), 7–15. *Accessed on 10 December 2021.* Retrieved from https://doi.org/10.22215/timreview/1174

Valtiohallinnon tietoturvallisuuden johtoryhmä. 2010. Sisäverkko-ohje. *Accessed on 9 January 2022.* Retrieved from https://www.suomidigi.fi/sites/default/files/2020-06/Ohje_3_2010_etusivu_ohjepdf.pdf

Baykara. 2020. PCI DSS Requirement 10 Explained. *PCI DSS GUIDE*. *Accessed on 20 December 2021.* Retrieved from https://www.pcidssguide.com/pci-dss-requirement-10/

Pescatore, J. (2021). *SANS 2021 Top New Attacks and Threat Report*. Accessed on 20 December 2021. Retrieved from https://www.sans.org/blog/sans-2021-threat-report/

Finnish Transport and Communication Agency. *2020. Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri). Traficom*. Accessed on 2 January 2021. Retrieved from https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/pilvipalveluiden-turvallisuuden-arviointikriteeristo-pitukri

Rapid7. n.d. A Definitive Guide to Understanding and Meeting the CIS Critical Security Controls. Accessed on 8 December 2021. Retrieved from https://www.rapid7.com/globalassets/_pdfs/whitepaper-guide/rapid7-solution-guide-a-definitive-guide-to-understanding-and-meeting-the-cis-critical-security-controls.pdf

Ministry of Finance. 2021. Recommendation on the handling of classified documents. Ministry of Finance. Accessed on 13 February 2022. Retrieved from https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162846/VM_2021_8.pdf?sequence=1

Refsdal, A., Solhaug, B., & Stølen, K. (2015). *Cyber-risk management*. Springer.

Brooks, R. 2020. Risk Analysis Example: How to Evaluate Risks. Netwrix. *Accessed on 10 December 2021.* Retrieved from https://blog.netwrix.com/2020/04/07/risk-analysis-example/

Rusere, K., & Ngassam, E. K. (2021). A Preliminary Integrated Network Security Framework for Tertiary Institutions. *2021 IST-Africa Conference (IST-Africa)*, 1–10. Accessed on 7 December 2021. Retrieved https://ieeexplore-ieee-org.ezproxy.jamk.fi:2443/stamp/stamp.jsp?tp=&arnumber=9576934&tag=1

The Rectors' Conference of Finnish Universities of Applied Sciences Arene. (2019.) Ethical recommendations for thesis writing at universities of applied sciences. Accessed on 21 February 2022. Retrieved from http://www.arene.fi/wp-content/uploads/Raportit/2020/ETHICAL%20RECOMMENDATIONS%20FOR%20THESIS%20WRITING%20AT%20UNIVERSITIES%20OF%20APPLIED%20SCIENCES_2020.pdf

Scarfone, K. A., Hoffman, P., & Souppaya, M. P. (2009). *Guide to enterprise telework and remote access security* (NIST SP 800-46r1; 0 p., s. NIST SP 800-46r1). National Institute of Standards and Technology. *Accessed on 12 December 2021.* Retrieved from https://doi.org/10.6028/NIST.SP.800-46r1

Shamma, B. 2018. Implementing CIS critical security controls for organizations on a low-budget. *Accessed on 26 December 2021.* Retrieved from https://uh-ir.tdl.org/bitstream/handle/10657/4048/SHAMMA-THESIS-2018.pdf?sequence=1&isAllowed=y

Souza, G. F. M. de, Caminada Netto, A., Melani, A. H. D. A., Michalski, M. A. D. C., & Silva, R. F. da. (2022). *Reliability analysis and asset management of engineering systems*.

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015). *Guide to Industrial Control Systems (ICS) Security* (NIST SP 800-82r2; s. NIST SP 800-82r2). National Institute of Standards and Technology. *Accessed on 10 December 2021.* Retrieved from https://doi.org/10.6028/NIST.SP.800-82r2

Liikenne- ja viestintävirasto kyberturvallisuuskeskus. 2019. Tunnetko jo PiTuKrin?. Traficom. *Accessed on 15 January 2022.* Retrieved from https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tunnetko-jo-pitukrin

Valtiohallinnon tietoturvallisuuden johtoryhmä. 2012. Teknisen ICT-ympäristön tietoturvataso-ohje. Vahti. *Accessed on 17 December 2021.* Retrieved from https://www.suomidigi.fi/sites/default/files/2020-06/VAHTI_3_2012_pdf.pdf

Valtiohallinnon tietoturvallisuuden johtoryhmä. 2003. *Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa.* Accessed on 3 February 2022. Retrieved https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet/vahti-72003-ohje-riskien-arvioinnista-tietoturvallisuuden-edistamiseksi-valtionhallinnossa

Itewiki. n.d. Viitekehyksiä parempiin tietoturvallisuuskäytäntöihin: Osa 2 – ISO/IEC 27001. *Accessed on 10 December 2021.* Retrieved from https://www.itewiki.fi/p/viitekehyksia-parempiin-tietoturvallisuus-kaytantoihin-osa-2-iso-iec-27001

Groot, J. 2021. What is PCI Compliance?. Digital Guardian. *Accessed on 13 December 2021.* Retrieved from https://digitalguardian.com/blog/what-pci-compliance

Balbix. n.d. What is the NIST Cybersecurity Framework? Accessed on 10 December 2021. Retrieved from https://www.balbix.com/insights/nist-cybersecurity-framework/

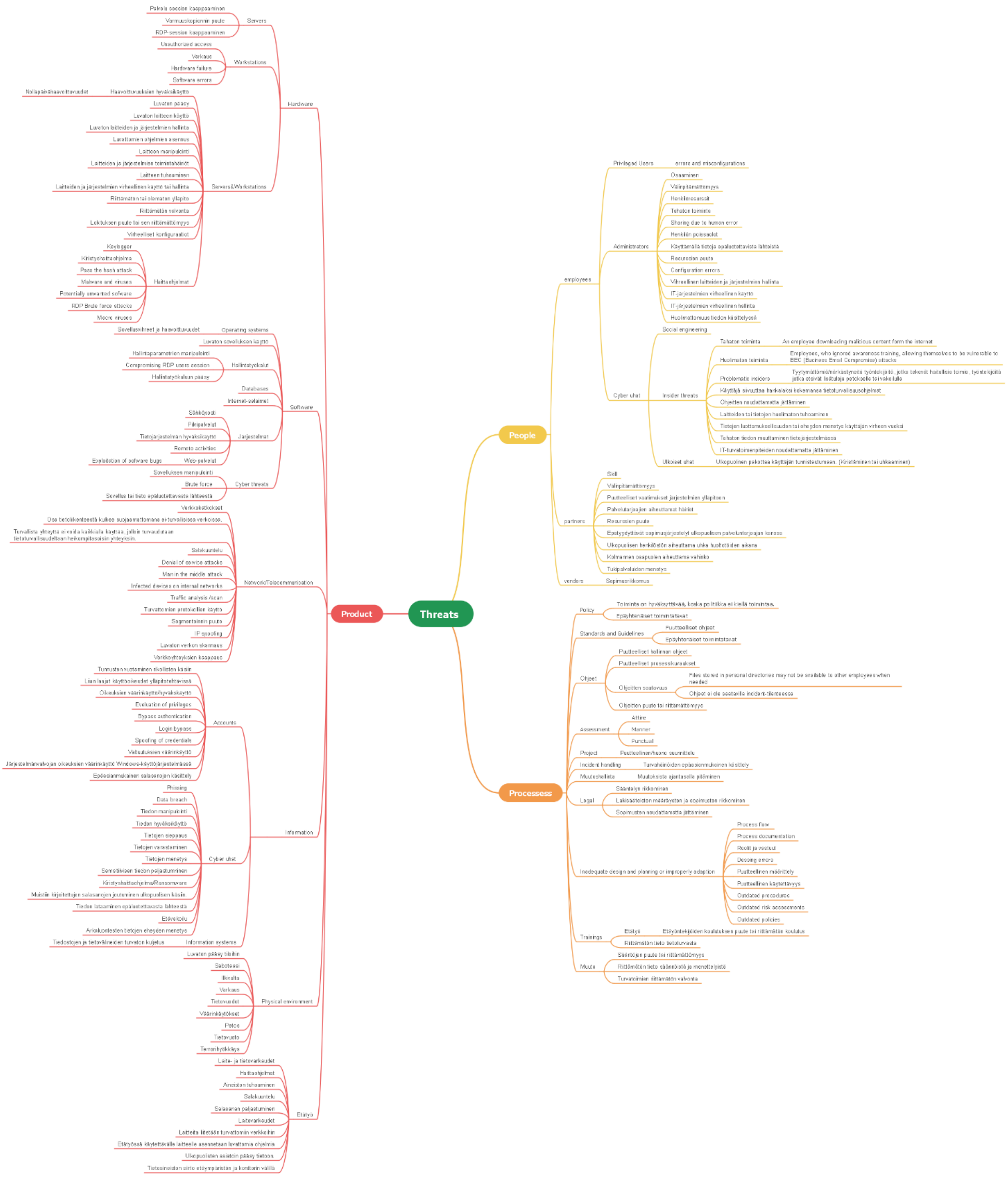
Williams, B. (2014). *Pci compliance: understand and implement effective pci data security standard compliance* (4th edition). Elsevier.

Appendices

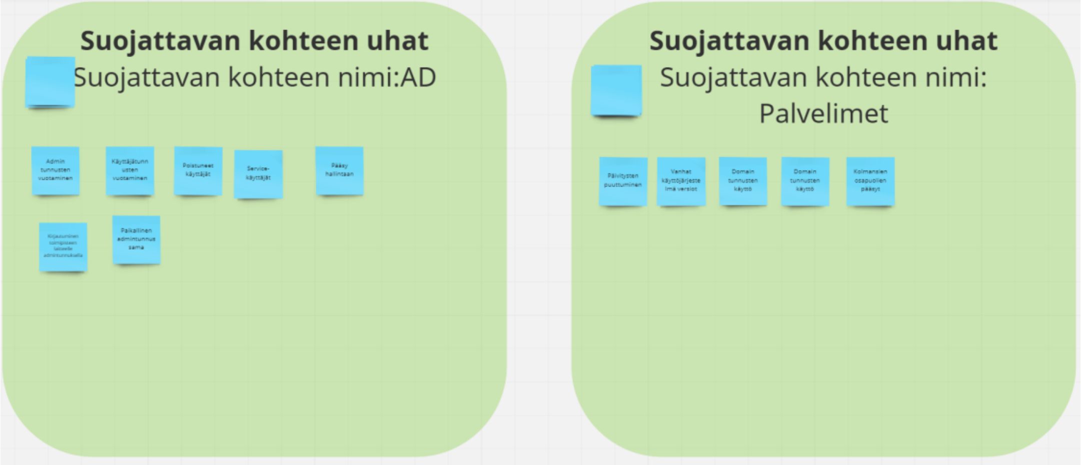
Appendix 1. Query

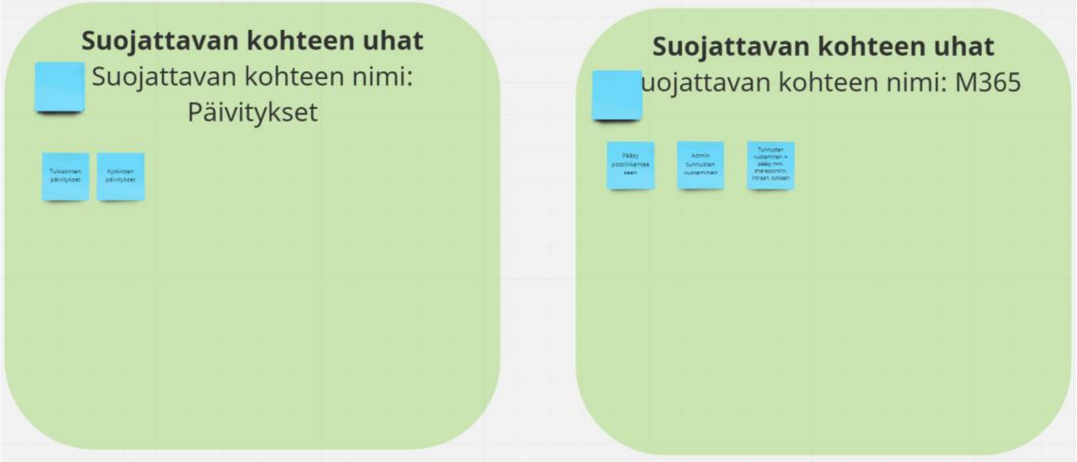
1. Käytätkö Domain Administrator -tunnusta työssäsi?
2. Mihin tarkoitukseen käytät Domain Administrator -tunnusta?
3. Kuinka usein käytät Domain Administrator -tunnusta työssäsi?
4. Mitä työkaluja käytät järjestelmien hallintaan omalla työkoneellasi?
5. Mitä työkaluja käytät eniten työkoneellasi? Lisää arvio kuinka paljon käytät työkalua viikossa.
6. Käytätkö toimistolla olevaa työkonetta järjestelmien hallintaan, kun olet etänä?
7. Millä etäratkaisulla otat yhteyden toimistolla olevaan koneeseen?
8. Mitä järjestelmiä hallitset toimistolla olevan työkoneesi kautta, kun olet etänä?
9. Kuinka usein suoritat järjestelmien hallintaa toimiston koneen kautta etänä ollessa?
10. Suoritatko järjestelmien hallintaa lääkäriaseman koneelta?
11. Mitä työkaluja käytät MGMT-palvelimella?
12. Mihin palvelimiin luot RDP-hallintayhteyksiä suoraan omalta työkoneeltasi?
13. Mihin palvelimiin luot RDP-hallintayhteyksiä MGMT-palvelimelta ja mitä tunnusta käytät kirjautumisessa? Kerro vapaasti.
14. Teetkö työssäsi tietokantakyselyjä?
15. Millä palvelimella tai työkoneella suoritat tietokantakyselyitä?
16. Mitä tunnuksia käytät tietokantapalveluun (SQL Server Management Studio) kirjautumisessa?
17. Kuinka usein suoritat tietokantakyselyitä?
18. Koetko, että organisaatiossa tarvitaan lisää turvallisuuskontrolleja, joilla voidaan parantaa IT-hallinnan tietoturvaa?
19. Kuinka tärkeänä pidät sitä, että tietoturva huomioidaan IT-asiantuntijan työssä?
20. Kuinka riittävänä koet oman osaamisesi ja tietämyksesi tietoturvaan liittyvissä asioissa?
21. Kaipaatko IT-järjestelmien hallintaan ohjeistuksia tietoturvan näkökulmasta ja yhtenäisempää toimintamallia?
22. Käytätkö työkonetta vapaa-ajallasi?

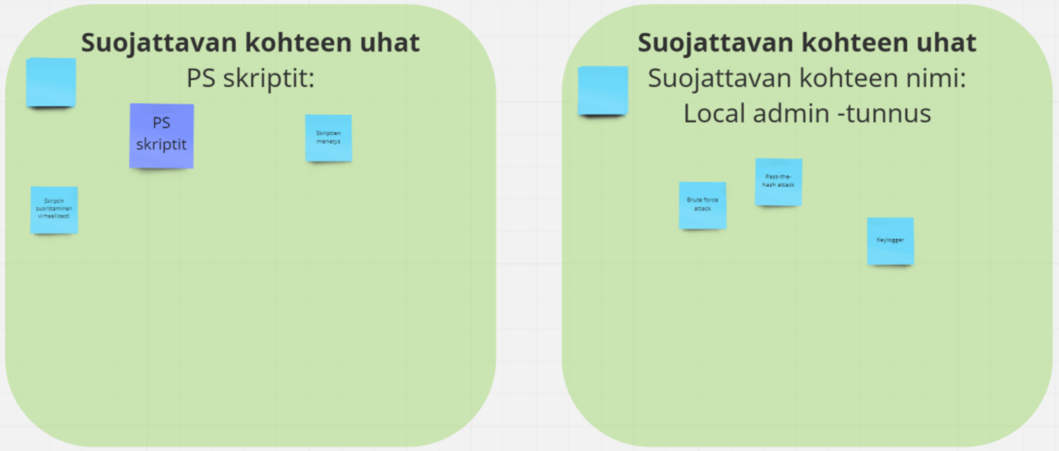
Appendix 2. Threat map that is classified in accordance with People, Process and Product principle

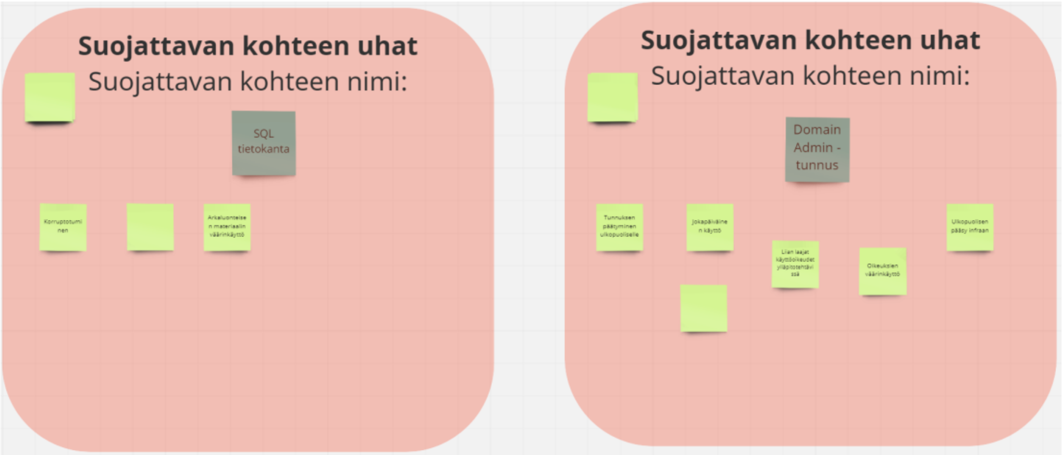

Threats
Product
Hardware
Servers
Paketu session kaappaaminen
Varmuuskopionnin puute
RDP-session kaappaaminen
Workstations
Unauthorized access
Varkaus
Hardware failure
Software errors
Servers&Workstations
Haavoittuvuuksien hyväksikäyttö
Nollapäivähaavoittuvuudet
Luvaton pääsy
Luvaton laitteen käyttö
Luvaton laitteiden ja järjestelmien hallinta
Luvattomien ohjelmien asennus
Laitteen manipulointi
Laitteiden ja järjestelmien toimintahäiriöt
Laitteen tuhoaminen
Laitteiden ja järjestelmien virheellinen käyttö tai hallinta
Riittämätön tai olematon ylläpito
Riittämätön valvonta
Lokituksen puute tai sen riittämättömyys
Virheelliset konfiguraatiot
Haittaohjelmat
Keylogger
Kiristyshaittaohjelma
Pass the hash attack
Malware and viruses
Potentially unwanted sofware
RDP Brute force attacks
Macro viruses
Software
Operating systems
Sovellusvihreet ja haavoittuvuudet
Luvaton sovelluksen käyttö
Hallintatyökalut
Hallintaparamatrien manipulointi
Compromising RDP users session
Hallintatyökaluun pääsy
Databases
Internet-selaimet
Jarjestelmat
Sähköposti
Pikipalvelut
Tietojärjestelmän hyväksikäyttö
Remote activities
Web-palvelut
Exploitation of sofware bugs
Cyber threats
Sovelluksen manipulointi
Brute force
Sovellus tai tieto epäluotettavasta lähteestä
Network/Telecommunication
Verkkokatkokset
Osa tietoliikenteestä kulkee suojaamattomana ei-turvallisissa verkoissa.
Turvallista yhteyttä ei voida kaikkiala käyttää, jolloin turvaudutaan tietoturvallisuudeltaan heikompitasoisin yhteyksin.
Salakuuntelu
Denial of service attacks
Man in the middle attack
Infected devices on internal networks
Traffic analysis /scan
Turvattomien protokollien käyttö
Segmentoinnin puute
IP spoofing
Luvaton verkon skannaus
Verkkoyhteyksien kaappaus
Information
Accounts
Tunnusten vuotaminen rikollisten käsiin
Liian laajat käyttöoikeudet ylläpitotehtävissä
Oikeuksien väärinkäyttö/hyväkskäyttö
Evaluation of privilages
Bypass authentication
Login bypass
Spoofing of credentials
Valtuutuksien väärinkäyttö
Järjestelmänvalvojan oikeuksien väärinkäyttö Windows-käyttöjärjestelmässä
Epäasianmukainen salasanojen käsittely
Cyber uhat
Phissing
Data breach
Tiedon manipulointi
Tiedon hyväksikäyttö
Tietojen sieppaus
Tietojen varastaminen
Tietojen menetys
Sensitiivisen tiedon paljastuminen
Kiristyshaittaohjelma/Ransomware
Muistiin kirjoitettujen salasanojen joutuminen ulkopuolisen käsiin.
Tiedon lataaminen epäluotettavasta lähteestä
Etävakoilu
Arkaluontesten tietojen eheyden menetys
Information systems
Tiedostojen ja tietovälineiden turvaton kuljetus
Physical environment
Luvaton pääsy tiloihin
Sabotaasi
Ilkivalta
Varkaus
Tietovuodot
Väärinkäytökset
Petos
Tietovuoto
Terrorihyökkäys
Etätyö
Laite- ja tietovarkaudet
Haittaohjelmat
Aineiston tuhoaminen
Salakuuntelu
Salasanan paljastuminen
Laitevarkaudet
Laitteita liitetään turvattomiin verkkoihin
Etätyössä käytettävälle laitteelle asennetaan luvattomia ohjelmia
Ulkopuolisten asiatoin pääsy tietoon.
Tietoaineiston siirto etäympäristön ja konttorin välillä
People
employees
Privilaged Users
errors and misconfigurations
Administrators
Osaaminen
Välinpitämättömyys
Henkilöresurssit
Tahaton toiminta
Sharing due to human error
Henkilön poissaolot
Käyttämällä tietoja epäluotettavista lähteistä
Resurssien puute
Configuration errors
Virheellinen laitteiden ja järjestelmien hallinta
IT-järjestelmien virheellinen käyttö
IT-järjestelmien virheellinen hallinta
Huolimattomuus tiedon käsittelyssä
Cyber uhat
Social engineering
Insider threats
Tahaton toiminta
An employee downloading malicious content form the internet
Huolimaton toiminta
Employees, who ignored awareness training, allowing themselves to be vulnerable to BEC (Buciness Email Compromise) attacks
Problematic insiders
Tyytymättömiä/närkästyneitä työntekijöitä, jotka tekevät haitallisia toimia, työntekijöitä jotka etsivät lisätuloja petoksella tai vakoilulla
Käyttäjä sivuuttaa hankalaksi kokemansa tietoturvallisuusohjelmat
Ohjeitten noudattamatta jättäminen
Laitteiden tai tietojen huolimaton tuhoaminen
Tietojen luottamuksellisuuden tai eheyden menetys käyttäjän virheen vuoksi
Tahaton tiedon muuttaminen tietojärjestelmässä
IT-turvatoimenpiteiden noudattamatta jättäminen
Ulkoiset uhat
Ulkopuolinen pakottaa käyttäjän tunnistautumaan. (Kristäminen tai uhkaaminen)
partners
Skill
Välinpitämättömyys
Puutteelliset vaatimukset järjestelmien ylläpitoon
Palvelutarjoajien aiheuttamat häiriöt
Resurssien puute
Epätyydyttävät sopimusjärjestelyt ulkopuolisen palveluntarjoajan kanssa
Ulkopuolisen henkilöstön aiheuttama uhka huoltotöiden aikana
Kolmannen osapuolen aiheuttama vahinko
Tukipalveluiden menetys
vendors
Sopimusrikkomus
Processess
Policy
Toiminta on hyväksyttävää, koska politiikka ei kiellä toimintaa.
Epäyhtenäiset toimintatavat
Standards and Guidelines
Puutteelliset ohjeet
Epäyhtenäiset toimintatavat
Ohjeet
Puutteelliset hallinnan ohjeet
Puutteelliset prosessikuvaukset
Ohjeitten saatavuus
Files stored in personal directories may not be available to other employees when needed
Ohjeet ei ole saatavilla incident-tilanteessa
Ohjeitten puute tai riittämättömyys
Assessment
Attire
Manner
Punctual
Project
Puutteelinen/huono suunnittelu
Incident handling
Turvahäiriöiden epäasianmukainen käsittely
Muutoshallinta
Muutoksista ajantasalla pitäminen
Lagal
Sääntelyn rikkominen
Lakisääteisten määräysten ja sopimusten rikkominen
Sopimusten noudattamatta jättäminen
Inadequate design and planning or improperly adaption
Process flow
Process documentation
Roolit ja vastuut
Dessing errors
Puutteellinen määrittely
Puutteellinen käytettävyys
Outdated procedures
Outdated risk assessments
Outdated policies
Trainings
Etätyö
Etätyöntekijöiden koulutuksen puute tai riittämätön koulutus
Riittämätön tieto tietoturvasta
Muuta
Sääntöjen puute tai riittämättömyys
Riittämätön tieto säännöistä ja menettelyistä
Turvatoimien riittämätön valvonta

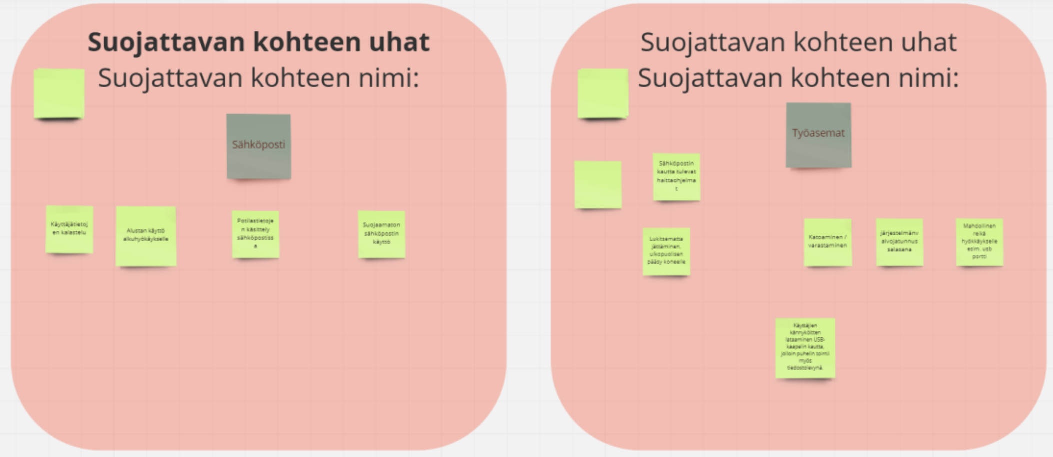
Appendix 3. The results of the identified assets to be protected and the threats

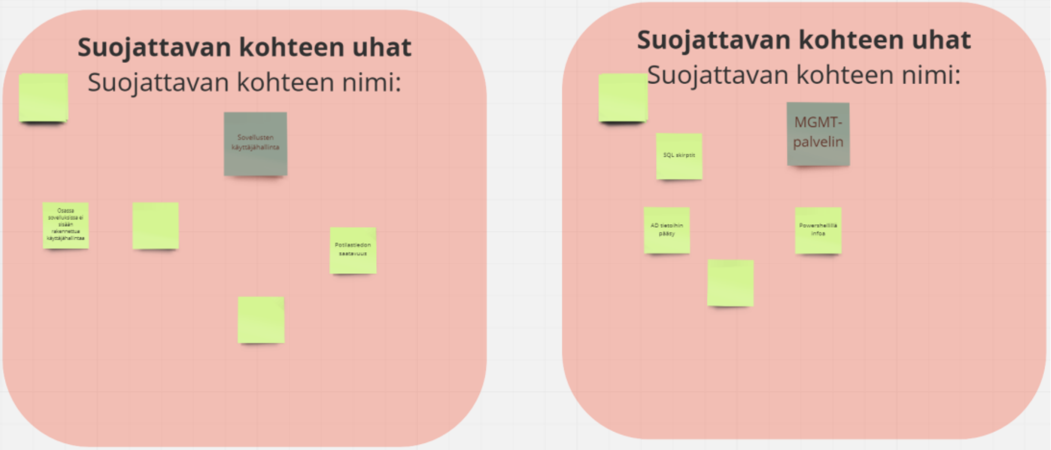

Suojattavan kohteen uhat
Suojattavan kohteen nimi:AD
Admin tunnusten vuotaminen
Käyttäjätunnusten vuotaminen
Poistuneet käyttäjät
Service-käyttäjät
Pääsy hallintaan
Kirjautuminen toimipisteen laitteelle admintunnuksella
Paikallinen admintunnus sama
Suojattavan kohteen uhat
Suojattavan kohteen nimi: Palvelimet
Päivitysten puuttuminen
Vanhat käyttöjärjestelmä versiot
Domain tunnusten käyttö
Domain tunnusten käyttö
Kolmansien osapuolien pääsyt


Suojattavan kohteen uhat
Suojattavan kohteen nimi: Päivitykset
Tulostimen päivitykset
Kytkinten päivitykset
Suojattavan kohteen uhat
uojattavan kohteen nimi: M365
Pääsy postiliikenteeseen
Admin tunnusten vuotaminen
Tunnusten vuotaminen -> pääsy mm. sharepointiin, intraan, tukaan


Suojattavan kohteen uhat
PS skriptit:
PS skriptit
Skriptien menetys
Skriptin suorittaminen virheellisesti
Suojattavan kohteen uhat
Suojattavan kohteen nimi:
Local admin -tunnus
Pass-the-hash attack
Brute force attack
Keylogger

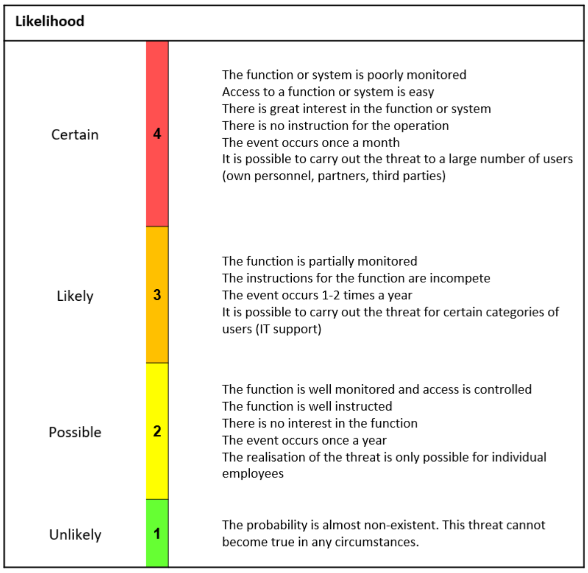

Suojattavan kohteen uhat
Suojattavan kohteen nimi:
SQL tietokanta
Korruptotuminen
Arkaluonteisen materiaalin väärinkäyttö
Suojattavan kohteen uhat
Suojattavan kohteen nimi:
Domain Admin -tunnus
Tunnuksen päätyminen ulkopuoliselle
Jokapäiväinen käyttö
Liian laajat käyttöoikeudet ylläpitotehtävissä
Oikeuksien väärinkäyttö
Ulkopuolisen pääsy infraan


Suojattavan kohteen uhat
Suojattavan kohteen nimi:
Sähköposti
Käyttäjätietojen kalastelu
Alustan käyttö aikuhyökkäykselle
Potilastietojen käsittely sähköpostissa
Suojaamaton sähköpostin käyttö
Suojattavan kohteen uhat
Suojattavan kohteen nimi:
Työasemat
Sähköpostin kautta tulevat haittaohjelmat
Lukitsematta jättäminen, ulkopuolisen pääsy koneelle
Katoaminen / varastaminen
järjestelmänvalvojatunnus salasana
Mahdollinen reikä hyökkäykselle esim. usb portti
Käyttäjien kännyköitten lataaminen USB-kaapelin kautta, jolloin puhelin toimii myös tiedostolevynä.

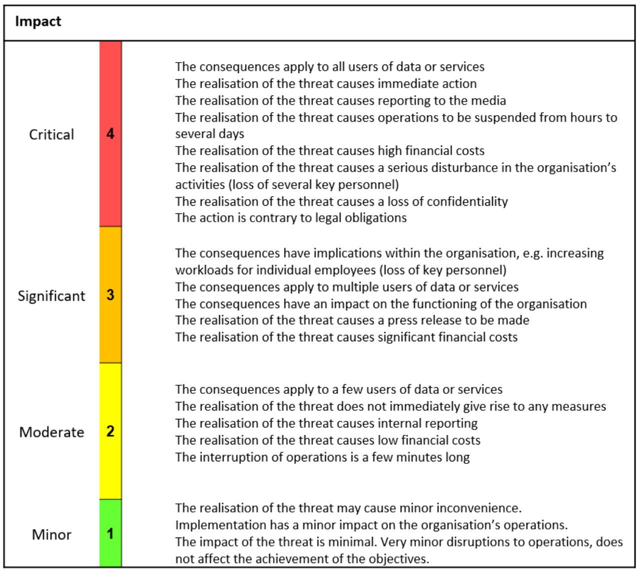

Suojattavan kohteen uhat
Suojattavan kohteen nimi:
Sovellusten käyttäjähallinta
Osassa sovelluksissa ei sisään rakennettua käyttäjähallintaa
Potilastiedon saatavuus
Suojattavan kohteen uhat
Suojattavan kohteen nimi:
MGMT-palvelin
SQL skirptit
AD tietoihin pääsy
Powershellillä infoa

Appendix 4. Classification of the likelihood and impacts of threats.

(Valtiohallinnon tietoturvallisuuden johtoryhmä, 2003, 41)



Likelihood		
Certain	4	The function or system is poorly monitored Access to a function or system is easy There is great interest in the function or system There is no instruction for the operation The event occurs once a month It is possible to carry out the threat to a large number of users (own personnel, partners, third parties)
Likely	3	The function is partially monitored The instructions for the function are incompete The event occurs 1-2 times a year It is possible to carry out the threat for certain categories of users (IT support)
Possible	2	The function is well monitored and access is controlled The function is well instructed There is no interest in the function The event occurs once a year The realisation of the threat is only possible for individual employees
Unlikely	1	The probability is almost non-existent. This threat cannot become true in any circumstances.



Impact		
Critical	4	The consequences apply to all users of data or services The realisation of the threat causes immediate action The realisation of the threat causes reporting to the media The realisation of the threat causes operations to be suspended from hours to several days The realisation of the threat causes high financial costs The realisation of the threat causes a serious disturbance in the organisation's activities (loss of several key personnel) The realisation of the threat causes a loss of confidentiality The action is contrary to legal obligations
Significant	3	The consequences have implications within the organisation, e.g. increasing workloads for individual employees (loss of key personnel) The consequences apply to multiple users of data or services The consequences have an impact on the functioning of the organisation The realisation of the threat causes a press release to be made The realisation of the threat causes significant financial costs
Moderate	2	The consequences apply to a few users of data or services The realisation of the threat does not immediately give rise to any measures The realisation of the threat causes internal reporting The realisation of the threat causes low financial costs The interruption of operations is a few minutes long
Minor	1	The realisation of the threat may cause minor inconvenience. Implementation has a minor impact on the organisation's operations. The impact of the threat is minimal. Very minor disruptions to operations, does not affect the achievement of the objectives.

Appendix 5. The risk categories and the actions

No risk	🟩	1-3	No acute measures are required, risk is at an acceptable level. Existing controls are functional.
Notable risk	🟨	4-6	Monitoring of the risk development is required; new controls are not needed at this stage.
Significant risk	🟧	8-9	Further planning is required to mitigate the risk. The mitigating measures to reduce or eliminate the risk will be taken care of during this budget period.
Intolerable risk	🟥	12-16	Immediate action is required for mitigating the risk.