UNIVERSITY
OF TURKU

Security Evaluation Methodology for Teaching and Learning Ecosystem

Master of Science (Tech) Thesis
University of Turku
Department of Computing
Communication and Cyber Security
Engineering
2023
Roope Pouta

Supervisors:
Seppo Virtanen
Mikko-Jussi Laakso

UNIVERSITY OF TURKU
Department of Computing

Roope Pouta: Security Evaluation Methodology for Teaching and Learning Ecosystem

Master of Science (Tech) Thesis, 51 p., 2 app. p.
Communication and Cyber Security Engineering
April 2023

In this thesis my research has focused on security evaluations and audits. How is a good security evaluation method made and what it includes. The purpose of this research is to create a suitable security evaluation methodology for learning ecosystems and test it in a case-study.

In the first two chapters I researched general information about already existing security evaluation methods and studies about security in learning platforms in general. What exactly are security evaluations and how those are used. In those chapters I also researched how to build a security evaluation method and then built one for the purpose of this thesis.

The last three chapters include the evaluation of the method and a case-study. Where the security evaluation method was tested. All of the requirements that are in the security evaluation method are inspected and also perfected in these chapters.

Digital learning platforms are becoming more and more popular. Because of the increasing user amount in said platforms security must be in a good order to protect its users. In my research I prove that security evaluations are necessary for learning ecosystems. There are no drawbacks to the organisation, they can only benefit from it. The case-study was conducted in Turku Research Institute for Learning Analytics (TRILA), where this method was found successful.

Keywords: Security Evaluation, Audit, Learning Ecosystem, Security Training

Contents

Appendices

1 Introduction

1.1 Purpose

In recent years especially during the pandemic e-learning platforms and learning ecosystems became much more relevant. During the sudden rush to e-learning platforms, security became an issue. Because of the increased development in user numbers security had to be re-evaluated to make sure that it was up to the required security standards [1].

The purpose of this thesis is to evaluate the security of the Turku Research Institute for Learning Analytics (TRILA). TRILA is an independent research institute working at the University of Turku. It employs roughly around thirty personnel currently. One of TRILA's objectives is to develop and maintain a digital learning platform called ViLLE, and to produce learning materials for it. TRILA is also heavily involved in research. Some of TRILA's research areas include: digital pedagogy, automatic evaluation of learning assignments, evaluation on effects of learning support, computational thinking, information management and teaching digitally in programming and languages. Also mathematical learning and teaching in a digital environment are part of their research endeavours.

Everything started in 2005 when the first version of ViLLE was published. At first ViLLE was a course project at university for code visualisation. But it had potential and started to grow into a learning platform that was used for teaching programming. The next step was to start producing ready to use educational materials for teachers, from which the ViLLE learning path was born. At first the focus was on creating mathematical materials for elementary schools. In 2015 native languages were implemented also to the learning path. In 2018 ViLLE started to create materials for computational thinking. All the content and technical planning is done with TRILA's partners. Centre for Learning Analytics was founded in 2016 and from 2022 onward TRILA has been operating as an independent unit. This is when the new name Turku Research Institute for Learning Analytics was applied.

In short TRILA's main purpose is to make education and learning better, with learning analytics. TRILA has won several awards but the biggest award was UNESCO King Hamad Bin Isa Al-Khalifa Prize for the use of ICT in Education in 2021.

TRILA has had a quite large impact on Finnish society. ViLLE learning platform is used in over half of the Finnish elementary schools, so TRILA is impacting Finnish students in their everyday life. There is also research evidence that using ViLLE improves learning and it helps teachers to keep better track of students progress and development.

1.2 Objectives and Research Methods

In this research the main goal was to create a suitable evaluation methodology for the purpose of evaluating the security of e-learning platforms and the organisation behind them. Objectives for this thesis are to develop security evaluation methodology and to use that method in a case-study to evaluate the security of TRILA. Also one of the objectives is to perfect all of the problems that occurred during the evaluation. This includes security training for the employees of TRILA.

TRILA's website did not offer enough information for my research about the institute therefore the first step going forward was to conduct a short interview with the coordinator in TRILA, which gave me insight into the institute (as presented in Appendix A). One of the objectives in the security evaluation was to evaluate all of the external and internal services that are used in TRILA. To get the information about those services, the leader of the development team was interviewed (as presented in Appendix B).

The problem when starting my thesis was that there were not any up-to-date methods for evaluating security of e-learning platforms. Therefore I created one for the purpose of this thesis. Katakri was used as a base for the evaluation method. Katakri is a Finnish national security audit criteria tool, which gives a set of requirements for authorities and organisations on how to achieve Finnish national security levels. Katakri covers information security and has divided it into three subdivisions: Security Management, Physical Security and Information Assurance [2].

Katakri was chosen to be the base for the evaluation method because of how broad it is. The method that was created during this thesis does not include all of the requirements that are set in Katakri, only the necessary for this research were collected from it. The selected requirements are based on the security issues that are present in e-learning platforms.

1.3 Structure

This thesis is divided into five main chapters. The first part of the research focuses on external and internal services in TRILA. This chapter goes through all of the external services that are used in TRILA. Also the focus is on what the services are and are they secure. Security Evaluations and Auditing has some background information about security evaluations, and how and why they are made for example.

The Security Evaluation Methodology chapter has information about how Katakri was chosen to be the base for the evaluation method. It also shows what other options there were and what are the guidelines that Katakri offers. The Implementation and Results chapter goes through all of the requirements that are listed in the Security Evaluation Methodology chapter. This chapter also shows the result of how TRILA fulfilled those requirements if it fulfilled them and if not why.

In the last chapter Actions all of the security requirements for TRILA that were not met are listed. It also shows what was done to fix those problems and how those requirements were fulfilled. The Actions chapter also goes through the security training that was developed during this thesis for the employees.

2 Security Evaluations and Auditing

2.1 Information About Evaluations and Auditing

In this chapter general information about evaluations and audits are being explained. So that in the later part of this thesis the reader has some kind of knowledge about evaluations and how they work. Also that when they are reading the requirements and results of the evaluation that is done in this thesis they understand the process behind it. The information that is explained in this chapter is collected and summarised from The ASQ Certified quality Auditor Handbook [3].

When evaluation or audit is done the evaluator is making observations and collecting data from those observations. Purpose of the evaluation is to verify that certain requirements are met. This is done by collecting hard evidence. Evaluations can be made against any set of standard requirements. Those can be governmental standards or just customer requirements. The only thing that is needed is a set of rules and it can be evaluated.

Evaluation can be done internally (first-party audit) or externally (second-, and third-party audit). Figure 2.1 demonstrates how each of these evaluation types work. A first-party audit is performed inside the organisation to make sure that all their procedures and methods are done correctly. A second-party audit is an external evaluation which is done by a customer to the supplier or by a contracted organisation for a customer. A second-party audits are usually more formal than first-party audits because the results might affect the customer's willingness to purchase the audits or not. This is why a second-party audit is subject to the rules of contract law. A third-party audit is performed by an organisation that is focused on doing audits. They are completely independent from the customer-supplier relationship thus are free of any conflicts.

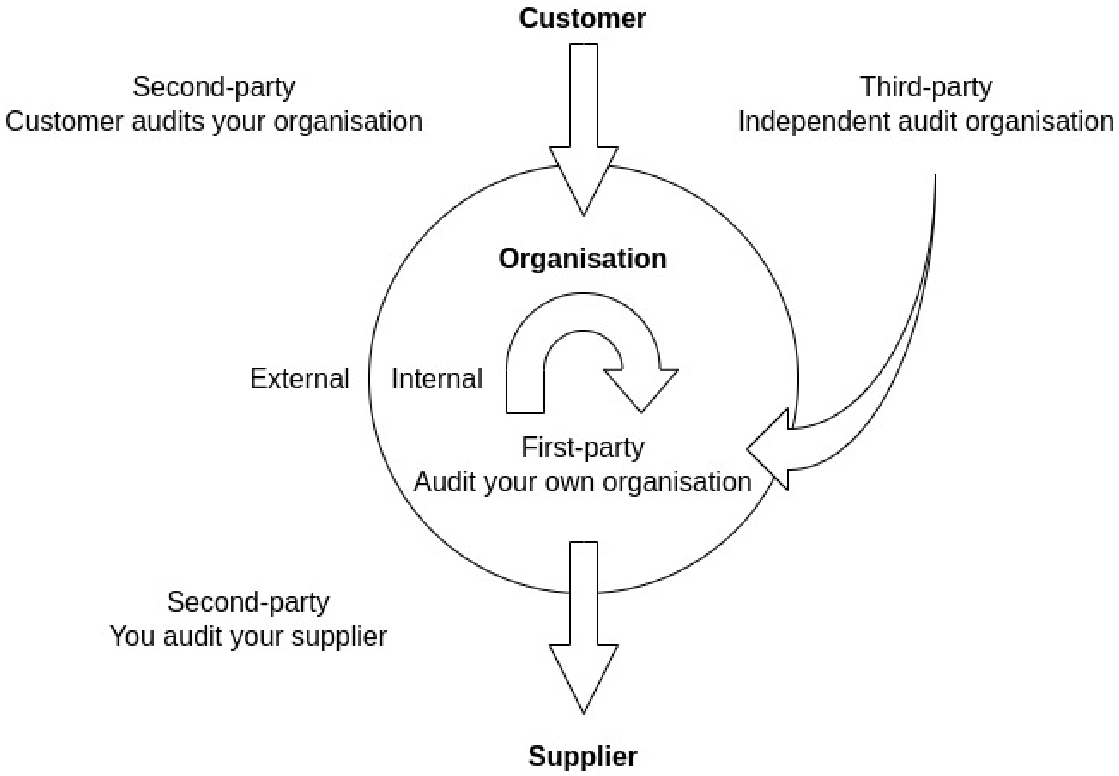


Figure 2.1: Evaluation types [3]

The main reason for evaluations is to improve the organisation. It can be about security, safety or for example effectiveness. There are a lot of regulations and requirements that come with products that organisations must follow to be able to sell those products. And the same applies for example the security side, when an organisation is handling classified information. In certain situations if organisations are not doing things by these regulations they can be fined. It is best for the organisation to make sure that everything is done by the book. Organisations also get more from the evaluations than a certainty that everything is done by the regulations. Usually something else comes up which might improve organisation's productivity or just make the day to day life easier.

These are the common elements that evaluation usually includes:

1. Purpose and scope
2. Document review
3. Preparation for review
4. On-site or remote data collection
5. Formal evaluation report
6. Evaluation follow-up

Evaluation process starts from defining the purpose and scope for the evaluation. Basically the answer for "Why are we doing this?" will provide the purpose and scope for the evaluation. Next step is to review documents to make sure that there are suitable documents for the evaluated area or activities to satisfy all requirements. Then comes preparation for the review, who will be interviewed and where. For example, is there something that needs to be scheduled. After all the preparations are done comes the evaluation itself, where the data is collected. When the audit is done, there is only the report that needs to be written. It is a formal document which has all the steps and procedures included. There is one last step that might be done and it is a follow-up after the evaluation. If there are a lot of things that did not pass the requirements in the original evaluation, the organisation is responsible for correcting all of these steps so that when the follow-up comes by they will pass it.

2.2 How to Build a Security Evaluation Method

There are a lot of evaluation and audit criterias and bases to choose from, so how do you know which is the best one for your purposes? It depends on the target of the evaluation and what kind of security risks might be involved in the organisation. Because there were no up-to-date audit criteria for learning ecosystems, in this thesis I will make an evaluation method exactly for that purpose and test it in case-study for TRILA.

So what does a good evaluation method include? There is an old evaluation method for virtual learning environments by M. Callejas-Cuervo and A. C. Alarcón-Aldana called “Security Evaluation Model for Virtual Learning Environments” [4]. In their model they start to build it from scratch, to see what makes a secure environment. They stated that to build a security evaluation model the most relevant security standards were to take into account. The criteria that was taken into account were: Confidentiality (C), Integrity (I) and Availability (A). These criterias are called the CIA triad. In the InfoSec handbook Umesh Hodeghatta Rao and Umesha Nayak states that “the CIA triad is one of the most important models of information security” [5]. The model specifies the important characteristics of information assets, and without them understanding information security is not possible. Meaning that when building an evaluation method the CIA triad has to be the foundation of it. The next step in the M. Callejas-Cuervo and A. C. Alarcón-Aldana paper was to evaluate the target organisations from the three perspectives that CIA triad offers and if all those areas were in good condition that meant that the organisation was secure.

Meghna Bhatia and Dr. J. K. Maitra wrote a paper called E-learning Platforms Security Issues and Vulnerability Analysis. In their paper they present a hierarchical approach for enforcing security in e-learning platforms as seen in the figure 2.2.

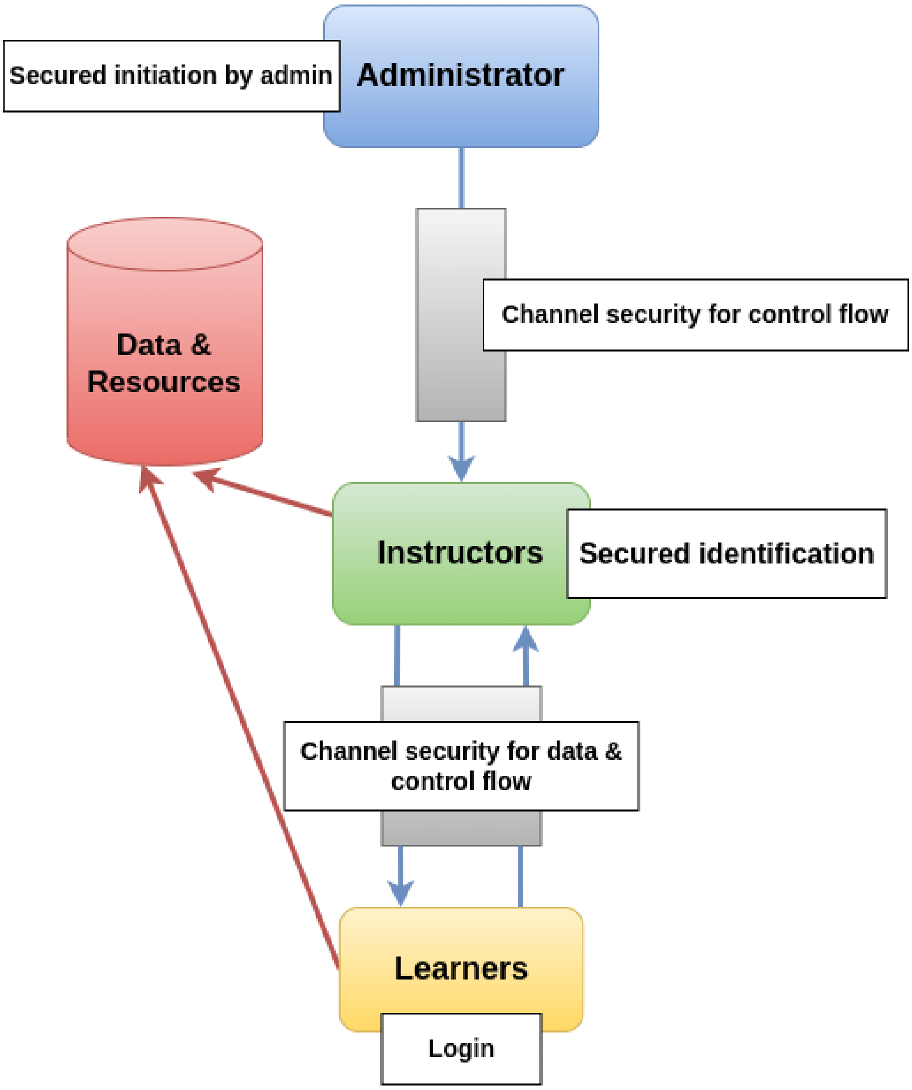

Secured initiation by admin
Administrator
Data & Resources
Channel security for control flow
Instructors
Secured identification
Channel security for data & control flow
Learners
Login

Figure 2.2: Enforcing security [6]

In this approach the security is enforced in a top-down manner. The reason for this type of security is that the monitoring could be done in a centralised manner and while enforcing security from the topmost level would certainly cover the entire system. In this approach the administrator initiates the security for the whole system. There is security in place between administrator and instructors which is perfect, because instructors should not have access to everything. However because instructors have access to some classified information, there is a secured identification system in place. Learners only have access to the assignments that instructors have made and there are security measures in place to prevent learners from accessing anything that they should not. There are some drawbacks to this type of security approach. If there are a lot of changes in the hierarchical structure in the organisation this approach would be hard to maintain [6]. But for the case-study which is done in this thesis this structure will work perfectly.

3 Security Evaluation Methodology

This chapter includes the guidelines which the security evaluation method for this thesis is made of. What are those guidelines, how it is used and what it actually includes. All of the requirements that the evaluation method will have are listed also in this chapter.

There are a lot of ways to do security evaluation for a learning ecosystem, some are more complex than others. Because this evaluation is needed for clients to showcase that all the systems are secure and the user data that is collected is handled correctly (according to GDPR). I decided to exclude ISO-standard referencing and chose to use tools that are made for security auditioning. Based on the findings in chapter Security Evaluations and Auditing I had two main options for the guidelines which to base my evaluation method on. Those were Katakri (Information security auditing tool for authorities) [2] and PiTuKri (Criteria to Assess the Information Security of Cloud Services) [7]. I chose to exclude PiTuKri from this evaluation method, because of the fact that Katakri covers everything that PiTuKri does and more.

Katakri also uses PiTuKri as a reference in many of the guidelines that are mentioned there. So there was no need for PiTuKri. Also cloud based technologies do not bring any new security risks, or the need to change the minimum controls to mitigate them, this is why PiTuKri is not needed. PiTuKri would have been great if this evaluation method would have only considered cloud services. The reason why I chose to use audition tools as a base for my method and not only reference ISO-standards was that when the client sees the document it is more readable. ISO-standards can get a little bit too confusing. Katakri gives a great base for the evaluation method, and thus makes it more understandable.

Even though this method is based on Katakri, it does not mean that when the evaluation is done the target of the evaluation is actually fully compliant with Katakri. Meaning that after the evaluation the target organisation will not get any certification from it. The method is made to give the organisations a set of guidelines which will lead them to the right path of cyber security. Also organisations will get a document that shows their clients that their security is up-to-date, even though it is not certified.

3.1 Katakri

Katakri is an information security audit tool for authorities made by the National Security Authority of Finland. It is a combination of the minimum requirements for security that are based on national legislation and international information security obligations. For this evaluation method Katakri is used from the perspective of learning ecosystem thus not all the Katakri's requirements and legislations are used. Katakri is divided into three subdivisions: security management, physical security and information assurance [2] .

All of the following legislations and regulations are based on the Katakri [2], which have been written in more readable and shorter form, also some excess information which isn't crucial for this evaluation method have been left out.

3.1.1 Security Management

Security management includes administrative level information security and personnel security. The aim of security management is to achieve a well functioning information management system, and to ensure that employees handle classified information in an appropriate manner. The processes that are included in security management should be handled as a whole concept. The way classified information is being handled should be determined by risk analysis, and based on that determine what to do with it.

What is included in good security management? First of all, documentation of practices and especially of risk management is a crucial part in good security management. All the plans and instructions should be provided in written format. Security management has been divided into two sub categories: administrative information security and personnel security. To use security management subdivision correctly on this evaluation, it has to be focused on the part of TRILA that handles classified information, in this case it is the whole institute.

Administrative Information Security

T - 01 - Support from the management, guidance, responsibilities - security principles

First section in the administrative information security category is: T - 01. It requires that organisations management is responsible for having security principles that are approved by senior management, where it is described how the security measures are linked to the organisations' activities. On top of that, security measures have to be appropriate for protecting classified information and that there is suitable monitoring in place to ensure that the organisation follows the requirements.

In general this means that the organisation has security principles approved by the top management, which indicates how security measures are connected to the organisations' actions. By doing this management shows that they are committed to the organisations security principles and express motivation of the management, while at the same time supporting organisations functions. Management is responsible for making sure that sufficient methods to ensure information security are in place. And that there is some kind of monitoring in place to ensure that those methods are being followed. It would also be good if the organisation describes how the monitoring has been organised to the management and supervisors and how its effectiveness is being monitored.

T - 02 - Defining the tasks and responsibilities of the security management

T - 02 requires that the tasks and responsibilities of security management have been defined. This section goes pretty much hand in hand with the first section, it has been only separated from it to more emphasis the fact that there must be a personnel who has been assigned to make sure that all the requirements are met and also that there is a employee who takes care of the maintenance of information security guidelines, risk management, preparedness and are generally responsible for the security of information.

T - 03 - Management of information security risks

T - 03 requires that the organisation has made assessments of the essential risks for classified information and made sure that the security measures are established accordingly. In general the management of information security risks is systematic, coordinated and continuous action, which is being used to analyse, estimate and handle security risks. The security risk handling process includes risk assessment, risk handling and risk monitoring.

T - 04 - Security guidance

T - 04 requires that the organisation has up-to-date instructions for handling classified information, how to use information systems and access rights to the classified information. These instructions cover the entire process of the information handling during the life cycle of the information. By documenting the essential information regarding the security, it ensures that the operation is not dependent on certain employees. Management is responsible for assessing a protocol which makes sure that the instructions stays up-to-date. For example assigning it to a certain employee. Usually it is somebody who has the knowledge of the whole picture of the organisation's security protocols.

T - 05 - Resources for the security work

T - 05 requires that the organisation has a certain level of expertise to ensure that security guidelines are being followed. In general this assures that the goal of information security will be achieved and the actions to mitigate risks are introduced in sufficient ways. Also it is regularly assessed that there are enough resources to achieve the goal of information security. The way to achieve this on a general level is to ensure that the organisation has enough employees who have knowledge and training in information security, up-to-date instructions, appropriate tools and that the organisation has organised the monitoring of security actions and inspections.

T - 06 - Malfunctions and exceptional situations

T - 06 requires that the organisation has made a plan on what to do in exceptional circumstances, in case of significant malfunctions or exceptional events. The plan must contain instructions on what to do in such situations, so that even if the key personnel cannot take action, other employees will understand the instructions. Also a key person must be defined who is in charge of protecting the classified information throughout the information lifecycle. Classified information must be protected against technological and physical accidents. In general organisations must have confidence that the classified information that they are handling or collecting, will be protected in the case of emergency or in disruptive situations. These situations might be fires, vandalism, break ins or just electronic malfunctions when devices break down. All the possible situations must have been thought of beforehand so that organisations can and know how to react when something goes wrong.

T - 07 - Management of security events

T - 07 requires that if an event occurs which has put classified information at risk, it has to be reported immediately to the security authorities. This also means that organisations have to have a plan in place to tell what to do in this kind of situation, as was mentioned in the T - 06. In this plan there are mentions about who are the key personnel, who must be informed at once and also what kind of security events have to be informed to the authorities.

Personnel Security

T - 09 - Changes in the handling of classified information throughout the employment

T - 09 requires that all the changes in the classified information are taken into account in all the different phases of employment. Especially organisations have to focus on recruitment, when responsibilities change and end of the employment contract. When new personnel are being employed an organisation needs to focus on security clearances, handling rights, rights to use and awareness for not sharing classified information. Also security training should take place when an employee starts, and to keep all of these updated when some changes occur. When a contract comes to an end, the organisation is responsible for making sure that all the keys, badges and classified information and material is handed over. On top of that all the access rights and rights to use should be removed. Also it would be good to remind the employee about the non-disclosure contract, because it will still apply even though the employee will not be working in the company anymore.

T - 10 - Assessment of the trustworthiness and reliability of the personnel

T - 10 requires that all the employees who are handling classified information should be checked for trustworthiness and reliability. If necessary organisations should do security clearance for the employee. If an organisation is handling data that has a high security level, then employees must have personnel security clearance for that certain level to get access to it.

T - 11 - Non-disclosure and confidentiality commitment

Non-disclosure contracts are in place when the person handling classified information doesn't have the responsibilities of an official. So when an organisation has even some kind of classified information, all the employees who get access to it must write a non-disclosure contract before getting the access. This will protect the information, because non-disclosure contracts are still in order even the employment contract comes to an end.

T - 12 - Security education

T - 12 requires that management has to make sure that employees are offered education, and to make sure that personnel and others working for the organisation have up-to-date knowledge of rules and regulations for handling classified information. Also employees should get educated about the threats against classified information. And if instructions change the updated information must be educated to the employees. It would be best to have regular training considering the handling of information. Management should also keep track of who participates in those.

T - 13 - Need-to-know and access rights

T - 13 requires that the organisation keeps track of all the employees who have access rights to the classified information. On that list there must be mentioned the employees task on which the right to handle classified information is based on. Employees can only get access to classified information when an individual's task-based need-to-know has been determined. Organisation should also have procedures in place to remove an employee's access rights when the need-to-know has ended. This ensures that employees who don't need to know the information anymore aren't just forgotten the access. It is much easier to determine the need-to-know when an organisation has described the principles to classified information and what the process includes when granting access to information. It should also be taken into account that when determining access rights, tasks and roles that dangerous role combinations are not created.

3.1.2 Physical Security

Physical security describes the required security for a physical environment where classified data is handled. Physical security is a combination of technical and physical security measures in order to prevent unauthorised access. Security measures are chosen from the risk evaluation that must be done. In this thesis I will make sure that the risk evaluation has been done, and the security measures are corresponding with that evaluation. Physical security has been divided into three categories: general requirements, requirements for security areas and requirements for data security.

General Requirements

F - 01 - Goals for physical security measures

F - 01 requires that there are appropriate physical security measures in place to prevent unauthorised access to classified information. This is done by making sure that classified information is being handled and stored in an appropriate manner. Granting access to classified information only on the need-to-know basis and that personnel have the required classification level, if that is needed. Deterring, preventing and detecting illegal actions and denying or trying to delay forced entry by intruders are goals for physical security.

F - 02 - Risk assessment of physical security measures

F - 02 requires that organisations have to assess all the risks and vulnerabilities for classified information on the premises. Selecting the physical security measures (F - 03) must be done based on the assessed risks. The assessment process has to take into account all the main factors:

1. Classification level of the information and the reason for confidentiality.

2. How the classified information is being handled and stored and also the size has to be taken into account. Because a large amount of information might need stricter security measures.

3. The time which classified information is being handled and stored.

4. Where the classified information is being stored, and the surroundings of that location.

5. How long is the reaction time in an emergency situation.

6. All the outsourced functions for example maintenance and cleaning.

F - 03 - Selection of physical security measures

F - 03 requires that in security areas and the surroundings, preventive actions have to be used to ensure the safety of the security areas. Actions to track and detect any harmful actions have to be included. Also there must be a procedure to recover normal functions immediately. Defence-in-depth principles must be used to determine sufficient security measures, based on the risk assessment, these are combined from physical, functional and administrative measures. Defence-in-depth means that multiple security measures are used on top of each other, which will complement each other. There are a lot of physical measures that can be used to ensure security, such as access control, intrusion detection systems, security personnel and security cameras.

F - 04 - Handling and storage of information

F - 04 requires that all the national classified information has to be handled in the security areas and in the surroundings so that the classified information is not accessible to unauthorised persons. The same goes for the international classified information. The three most common classification levels are: restricted, confidential and secret.

Requirements for Security Areas

F - 05 - Administrative area

F - 05 requires that the area has a clearly defined and visible boundary, but there aren't any requirements for the structure that is setting the boundary. In this case administrative area means areas and spaces that are planned for normal working conditions, for example offices. It also requires that the access rights are only given to authorised personnel. Organisations must define procedures and roles for access rights, including physical key management. Everytime that people who are not authorised come to visit they must have an escort. Soundproofing is also one requirement regarding the structures. Soundproofing must be made so that unauthorised people cannot hear conversations about classified information. This also applies inside the organisation if there are different levels of authorisations between employees. Also if there is a risk that classified information might be seen through unauthorised observation, for example working in public transports, then measures to prevent that must be in place. Organisations must make sure that classified information or the devices that contain said information is being stored according to the corresponding information classification level.

Requirements for Data Security

F - 08 - Data security

F - 08 lists the requirements for handling classified information in paper format. Whenever classified information is being transported it must be done according to the instructions given by the organisation, while simultaneously following the necessary protective measures. Information must be packed so that it prevents any unauthorised disclosure. When copying classified information, the security measures that apply to the original document, will also apply to the copies and translations. When disposing of classified material, it has to be done so that it prevents reconstruction of the information, for example paper shredder.

3.1.3 Information Assurance

Information assurance provides security requirements when handling classified information in electronic format. In the case of TRILA, security measures only have to meet the standards for RESTRICTED (national classification level IV). Information assurance has been divided into three categories: communications security, systems security and operations security.

Communications Security

I - 01 - Secure interconnection of information processing environments - Security of the network architecture

I - 03 requires that the information processing environment is excluded from the other environments. When connecting the information processing environment to another environment which is handling classified information it requires at least the use of a firewall. Excluding the information processing environment from other environments is the most effective way to protect classified information. Also when the classified information is in one place it is more easily managed and protected.

I - 02 - Principle of least privilege - Segmenting of the communication network and filtering rules within the classification level

I - 02 requires that communication network segmentation and filtering must be done by following the principles of least privilege and defence-in-depth. Basically the division of communication networks may mean that you separate the workstation and servers, also it applies the separation needs in individual projects. Way of implementing this requirement is to divide the network into separate areas within the classification level. By default traffic between network areas is denied, only pre-authorised and essential information for the operation is allowed.

I - 03 - Security of information processing environment throughout the life cycle - management of filtering and monitoring systems

I - 03 requires that appropriate filtering and monitoring systems are taken care of trough-out the whole life cycle of the information-processing environment. Tasks are given to make sure that any changes in the setup of filtering and monitoring systems are taken into account. Documentation of the network and its filtering and monitoring systems is maintained through its life cycle.

I - 05 - Exchange of classified information outside the physically protected areas - wireless transmission

I - 05 requires that wireless transmissions are encrypted with a solution that is appropriate for the classification level of the information.

Systems Security

I - 06 - The principle of least privilege - management of access rights

I - 06 - requires that user rights to information systems have been defined and issued if employees have the rights to handle the information. User rights have to be maintained and updated when needed. In general the main objective of management of access rights is to make sure that only authorised users have access to the information-processing environment.

I - 07 - Defence-in-depth - identification of actors of the information processing environment within a physically protected security area

I - 07 requires that all the employees, devices and systems that are using the information-processing environment are identified reliably enough. In general users must have personal identifications and all the users are identified and authenticated.

I - 08 - Principle of minimality and of least privilege - systems hardening

I - 08 requires that only the essential functions are implemented to avoid unnecessary risks. Organisations must have procedures where systems are installed and configured so that it results in hardened installation. Hardened installation includes only mandatory components and process rights so it fulfils the security requirements.

I - 09 - Defence-in-depth - protection against malware

I - 09 requires that sufficient methods are in place to prevent unauthorised changes in the information processing environment. In general this can be achieved with multiple methods, for example with the system hardening (I -08) and limitations in user rights (I - 06).

I - 10 - Defence-in-depth - Traceability of security events

I - 10 requires that an organisation must have reliable methods for tracing security events in order to detect unauthorised changes within the information processing environment. When using information systems, disclosure of their information must be logged in case the use of the classified information requires identification. The log is to keep track of where the information is used and to find out why some technical failures occur.

I - 11 - Defence-in-depth - incident detection and recovery

I - 11 requires that reliable methods are in place to detect attacks and limit the effects of that attack against the information processing environment and also to restore the protected status as fast as possible.

I - 13 - Defence-in-depth throughout the life cycle - protection of software against network attacks

I - 13 requires that security of the information processing environment is tested during the accreditation process to ensure that the security is at the appropriate level and that it is correctly implemented. Also protective measures must be in place against network attacks and those protective measures are taken care of throughout the whole life cycle of the information processing environment.

Operations Security

I - 15 - Exchange of classified information between physically protected areas - electronic transfer of the information

I - 15 requires that when classified information is being transferred outside physically protected areas, the information must be encrypted.

I - 16 - Security throughout the information processing environment life cycle - change management

I - 16 requires that security must be required throughout the information processing environments life cycle. All the security inspections, reviews and assessments must be performed periodically when maintaining the information processing environment and also if something exceptional arises.

I - 18 - Handling and transfer of classified information between physically protected areas - remote use and remote management

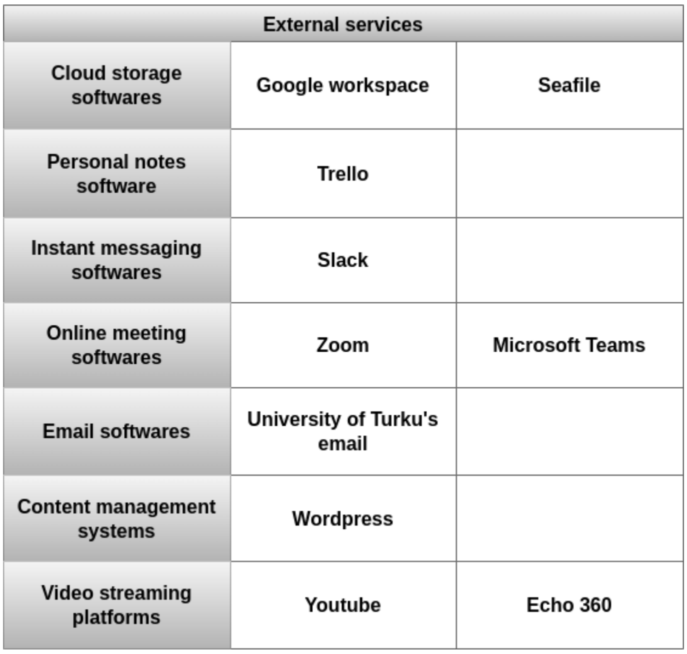
I - 18 requires that when classified information is being handled outside of security areas, it must be done so that unauthorised access is prevented and personnel have been trained to secure remote work. If devices that contain classified information have not been encrypted, that device must be on constant surveillance. When using these devices remotely, appropriate precautions must be taken into account.

4 External Services And TRILA

As an institute which employs about 30 personnel TRILA uses a great deal of different services. This chapter will go through each of those services and why exactly that service is selected and where it is used. Information about these services are collected from multiple conversations with Juho Kuusinen who is the leader of the developer team in TRILA. Those services are listed here below. As a base for the conversations I have used interview questions that are listed in Appendix B.

4.1 External Services

Google Workspace is a platform which includes a combination of multiple softwares that are developed by Google. For example those softwares are collections of cloud computing, productivity and collaboration tools, which includes for example Google Drive and Gmail. When it comes to the security side of Google Workspace, it is certified as ISO/IEC 27001 compliant, which means that it is up to the methods standards which were made in chapter Security Evaluation Methodology [8]. TRILA chose to transfer to Google Workspace, because of how easy it is to manage information in it. Before Google Workspace TRILA was using multiple different shared drives, but with Google Workspace all of those could be combined and are now in the same place. Also for TRILA it is useful that you can easily assign different roles for people or grant different permissions for different employees, so that not everybody can see every file and project in it. This is needed because of the safety



External services		
Cloud storage softwares	Google workspace	Seafile
Personal notes software	Trello	
Instant messaging softwares	Slack	
Online meeting softwares	Zoom	Microsoft Teams
Email softwares	University of Turku's email	
Content management systems	Wordpress	
Video streaming platforms	Youtube	Echo 360

Figure 4.1: External services used in TRILA

that comes when information is shared only on a need-to-know basis.

Trello is a web-based application where you can create your own to-do lists. From the security point of view it does not matter because there is not any information saved that actually would need to be secure. Nonetheless Trello is secure enough to pass the methods standards which were made in chapter Security Evaluation Methodology [9]. Trello is barely used in TRILA, because the general instructions do not recommend its usage. Nonetheless, there are still some employees who use it. Mostly those employees use it to organise their personal work assignments.

Slack is a messaging application that is designed to be used in the office. In Slack you can have personal conversations but also group discussions that are limited to only people who have been granted access. Slack has achieved ISO 27001 and ISO 27018 compliance, which then fulfils the methods standards which were made in chapter Security Evaluation Methodology [10]. Slack was selected to be the main messaging application inside of TRILA because most of TRILA's partners are using it. This allows conversations inside projects over different organisations. There were few different options where to choose from, for example Microsoft Teams and Mattermost. TRILA's management rejected Teams as a messaging platform, and with Mattermost there were problems because it is wholly managed by University of Turku, so for example having private channels became a problem.

Microsoft Teams is a business communication platform developed by Microsoft. From the security side of things, Teams is a very secure platform and thus it is up to the methods standards which were made in chapter Security Evaluation Methodology [11]. In TRILA Teams are only used sometimes when partners insist on having remote meetings. Despite Microsoft Teams being a secure platform TRILA is not using it for their own online meetings. This is because the management doesn't support Microsoft Teams usage. And have chosen to use different applications for remote meetings.

Zoom is a communications technology company which provides online chat services and it is mostly common for video conferencing [12]. TRILA has chosen to use Zoom as an online meeting platform, because of its ease of use and many functionalities, for example break out rooms. Mostly TRILA uses Zoom to have meetings with employees from TRILA's partners. In these meetings nothing classified information is shared, but Zoom still has good enough security measures for TRILA.

Github is an internet hosting and version control service for developers using Git. From the security side of things Github is certified by ISO 27001, so it fulfils the methods standards which were made in chapter Security Evaluation Methodology [13]. Basically Github is a webpage that allows you to organise and easily keep track of your projects and all the steps that are included in the development of said projects. For example different branches and issues. TRILA moved from Gitlab (which is a similar application than Github) to Github because of some issues with local instances. Github also allows TRILA to easily work with Eduten (Eduten is the commercialised version of ViLLE). TRILA mostly uses Github to develop ViLLE and keep track of issues regarding it.

University of Turku's email is the university's hosted microsoft exchange service. University of Turku's email is also ISO 27001 certified, thus it fulfils the methods standards which were made in chapter Security Evaluation Methodology [14]. TRILA uses University of Turku's email because they are under the University of Turku. It is also convenient that all the internal emails are sent automatically via secure email. This allows a secure way to transfer information between researchers.

WordPress is a free content management system which is written in hypertext preprocessor language and paired with a MySQL or MariaDB database with supported HTTPS. From the security side of things WordPress also has a ISO 27001 certification, thus it fulfils the methods standards which were made in chapter Security Evaluation Methodology [15]. TRILA's webpage was chosen to be created with WordPress because of how easily you can manage its content also without the developers. Colibri is a theme in WordPress that was chosen for TRILA's webpage because the developer preferred it.

YouTube is a platform for online video sharing. For the security side the same applies to YouTube than Google Workspace because both are owned by Google. Therefore YouTube also fulfils the methods standards which were made in chapter Security Evaluation Methodology [16]. TRILA uses YouTube for sharing different kinds of video materials. The reason why YouTube was selected is because of how easily you can maintain your materials and update them, for example adding subtitles. Also YouTube makes it quite easy to share the material with other users.

Echo 360 is a platform used for lectures [17]. The security of Echo 360 does not really matter since there are only some educational videos there. However it complies with General Data Protection Regulation (GDPR) so it fulfils the methods standards which were made in chapter Security Evaluation Methodology. When TRILA was still giving some software developer lectures Echo 360 was used for sharing some materials, but it is barely used anymore. There might still be some lecture materials that are stored there but other than that it is not used.

Seafile is an open source platform for file syncing, hosting and sharing. Because Seafile is a self-hosted file sharing platform it works well for private cloud applications like University of Turku [18]. University of Turku has their own personalised Seafile solution, which allows them to make sure that the security of the cloud application is on the correct level. TRILA uses Seafile for storing the most classified information. In this case the research data which have personal information. TRILA has chosen to use this because it is the most secure place to store information that the University of Turku offers.

4.2 Internal Services

There are a few internal services that TRILA provides. These are Functional Numeracy Assessment (FUNA)-analytics service and knowledge management service. The FUNA-analytics service handles data and gives the values corresponding to FUNA-testings. FUNA-analytics service is secure in terms of personal information. It handles course, round and userID information, which all are protected by hashing. To get some data out of the analytics service you have to know the owner of the data and the corresponding hash to it. On top of that you have to have access to ViLLE in order to get anything out of it. ViLLE is also the system that does the hashing for the information.

The knowledge management service is a service that displays primus-data from where the local headmasters and head of the local education and culture department can see how certain groups of people are doing. For example you can view how grade 5A is compared to class B. There is no personal information shown, the service only knows the studentID which is secured by hashing. The service also does not show individual performance, only classroom or grade level or even broader scale information.

Because both of these services are done so securely there is not any concern that they could bring any security weaknesses to TRILA. Both services are working in intranet's intranet, so there is not actually any risk of anybody getting in. On top of that there are all the precautions that are included in University of Turku systems. Basically both services are to showcase data in some kind of form without giving any sensitive information away.

5 Implementation And Results Of The TRILA Security Evaluation

This chapter includes the case-study where I test the evaluation method that was made in chapter Security Evaluation Methodology to evaluate TRILA's security. All of the chapter's requirements are once again gone through, but this time from TRILA's perspective. If all of the requirements are met and if not then why.

Information that is referenced with tools that are explained in chapter Security Evaluation Methodology, is gathered by conducting interviews with employees of TRILA and the University of Turku's head of security. Main focus with the interview questions is to gather all the information about TRILA's systems and data handling and reference those with the evaluation method that was made.

5.1 Security Management

5.1.1 Administrative Information Security

T - 01 - Support from the management, guidance, responsibilities - security principles

The requirements that are required by T - 01 are present in the organisation and approved by the senior management as required. In TRILA's case there are two different sets of security principles: the one that is in TRILA and the other in

University of Turku.

T - 02 - Defining the tasks and responsibilities of the security management

The requirements that are required by T - 02 are present in the organisation. Security responsibilities are being managed from the University of Turku's Digital Services. It would be good that TRILA had its own security personnel inside of the organisation, so it could manage the security in day-to-day life. Although this is not required, it would make a difference in the security aspects of the organisation.

T - 03 - Management of information security risks

The requirements that are required by T - 03 are present in the organisation. Risk management is done by the University of Turku's Digital Services, where they are following their security policies and managing security risks case by case. Risk evaluation is done when certain systems have been developed and security is done according to that evaluation.

T - 04 - Security guidance

The requirements that are required by T - 04 are partially present in the organisation. Meaning that the organisation has instructions regarding the handling of classified information, but they are not updated, and some minor details might be missing. Also these instructions could be more available for employees.

T - 05 - Resources for the security work

The requirements that are required by T - 05 are present in the organisation. University of Turku's security management makes sure that security guidelines are being followed. But it would be good if TRILA had its own security personnel who would manage this inside the organisation, and make sure that security guidelines are being followed in day-to-day life.

T - 06 - Malfunctions and exceptional situations

The requirements that are required by T - 06 are present in the organisation. University of Turku's Digital Services has guidelines on how to proceed in exceptional situations. On top of that they have done the preventing security measures when certain systems have been developed. Also TRILA has their own guidelines on how to proceed in GDPR incidents.

T - 07 - Management of security events

The requirements that are required by T - 07 are present in the organisation. Guidelines on how to proceed in case of security breaches are listed on University of Turku's website. Also, the University of Turku's Digital Services has internal guidelines on how to proceed after something has come up and how to prevent events from escalating.

5.1.2 Personnel Security

T - 09 - Changes in the handling of classified information throughout the employment

The requirements that are required by T - 09 are present in the organisation. Meaning that all the changes throughout the employment have been taken into account considering the handling of classified information.

T - 10 - Assessment of the trustworthiness and reliability of the personnel

The requirements that are required by T - 10 are present in the organisation. Reliability is being assessed by the organisation's management when conducting the interviews. This fulfils the requirements because TRILA does not handle national classification level of information.

T - 11 - Non-disclosure and confidentiality commitment

The requirements that are required by T - 11 are present in the organisation. There are multiple non-disclosure agreements that are written. One when signing the contract with University of Turku, and then developers also sign one of their own. There also could be one specific with TRILA just to simplify this more, but it is not necessary.

T - 12 - Security education

The requirements that are required by T - 12 are not present in the organisation. Meaning that there is not currently any security education. This will be fixed while writing this thesis. There will be a separate chapter for the security education.

T - 13 - Need-to-know and access rights

The requirements that are required by T - 13 are present in the organisation. Access rights are given on the need-to-know basis. There are also logs where you can see these access rights. The documentation of those access-rights could be better. The documentation should contain all the access rights and need-to-know basis that each employee has.

5.2 Physical Security

5.2.1 General Requirements

F - 01 - Goals for physical security measures

The requirements that are required by F - 01 are present in the organisation. In the TRILA's office there are multiple ways in place to achieve goals for physical security measures.

F - 02 - Risk assessment of physical security measures

The requirements that are required by F - 02 are present in the organisation. The risk assessment of the security measures are done by the University of Turku's Digital Services.

F - 03 - Selection of physical security measures

The requirements that are required by F - 03 are present in the organisation. Defence in depth is being achieved with multiple security measures that are selected to cover all the points that came up in the risk assessment in F - 02.

F - 04 - Handling and storage of information

The requirements that are required by the F - 04 are present in the organisation. Everytime that classified information is being handled it is done properly and the storage of said information is also done securely.

5.2.2 Requirements for Security Areas

F - 05 - Administrative area

The requirements that are required by the F - 05 are present in the organisation. Meaning that TRILA has a specified office space where only authorised personnel can enter. Also the office has sound proofed spaces where employees can discuss classified information without being overheard by people who do not have access to said information.

5.2.3 Requirements for Data Security

F - 08 - Data security

The requirements that are required by the F - 08 are present in the organisation. Although the amount of information that is being handled in paper format is very minimal the required safety measures have been taken into account, considering storing, transporting and disposing it.

5.3 Information Assurance and GDPR

5.3.1 Communications Security

I - 01 - Secure interconnection of information processing environments - Security of the network architecture

The requirements that are required by I - 01 are present in the organisation. The information processing environment has been divided into separate zones and the security is centralised.

I - 02 - Principle of least privilege - Segmenting of the communication network and filtering rules within the classification level

The requirements that are required by I - 02 are present in the organisation. The information processing environment has been segmented and the filtering rules have been done correctly. Meaning that all the necessary aspects have been taken into account, for example defence-in-depth.

I - 03 - Security of information processing environment throughout the life cycle - management of filtering and monitoring systems

The requirements that are required by I - 03 are present in the organisation. All of the required steps have been taken into account and documented. This is done by the University of Turku's Digital Services.

I - 05 - Exchange of classified information outside the physically protected areas - wireless transmission

The requirements that are required by I - 05 are present in the organisation. Everytime classified information is being transmitted it is protected. It is transmitted via secure email or if necessary the file is also protected with password, and sent in separate email.

5.3.2 System Security

I - 06 - The principle of least privilege - management of access rights

The requirements that are required by I - 06 are present in the organisation. Access to classified information is only given when needed and removed after that. The document that was mentioned in T - 13 will be supporting this and making this more clearer and easier to manage.

I - 07 - Defence-in-depth - identification of actors of the information processing environment within a physically protected security area

The requirements that are required by I - 07 are present in the organisation. You can not see any information inside of TRILA without identification. On top of that all the access to classified information is backed up with two factor authentication.

I - 08 - Principle of minimality and of least privilege - systems hardening

The requirements that are required by I - 08 are present in the organisation. All the computers that TRILA's employees are using come from the University of Turku's Digital Services, where all the necessary systems and appliances are installed and access to systems that might cause vulnerabilities in the device are blocked by the Digital Services.

I - 09 - Defence-in-depth - protection against malware

The requirements that are required by I - 09 are present in the organisation. All of the needed procedures are also documented in the University of Turku's Digital Services.

I - 10 - Defence-in-depth - Traceability of security events

The requirements that are required by I - 10 are present in the organisation. I can not go into more details because it is classified.

I - 11 - Defence-in-depth - incident detection and recovery

The requirements that are required by I - 11 are present in the organisation. There are procedures in place to prevent and detect unwanted actions. I can not go into more details because it is classified.

I - 13 - Defence-in-depth throughout the life cycle - protection of software against network attacks

The requirements that are required by I - 13 are present in the organisation. All of the needed procedures are done. I can not go into more details because it is classified.

5.3.3 Operations Security

I - 15 - Exchange of classified information between physically protected areas - electronic transfer of the information

The requirements that are required by I - 15 are present in the organisation. When classified information is being transferred, it is being sent through secure email and encrypted with password, which is given separately. This ensures that the information is being accessed only by the people who were meant to access it.

I - 16 - Security throughout the information processing environment life cycle - change management

The requirements that are required by I - 16 are partially present in the organisation. All the critical aspects of the security infrastructure are being checked and evaluated periodically. But it would be good that inside of TRILA there would also be some kind of security evaluations periodically.

I - 18 - Handling and transfer of classified information between physically protected areas - remote use and remote management

The requirements that are required by I - 18 are present in the organisation. If somebody is working in a public setting they can get the security protector for their screen, other than that people are sometimes working from home, but classified information is not being handled in public.

6 Actions

This chapter will include what actions have been made towards the sections that needed some improvements to meet the requirements set by the evaluation method. There was not anything alarming or crucial that was missing, but some little things that will make security easier and more secure in day-to-day life in TRILA. These improvements are listed one section at a time, to keep the same concept that has been used in the thesis earlier, so it is easier to read and refer to the requirements for each section. All of the actions below will be taken into action immediately while writing this thesis.

6.1 Security Improvements

T - 02 - Defining the tasks and responsibilities of the security management

T - 02 required that there is defined personnel who handles the security aspects of the organisation. In TRILA's case this is handled from the Digital Services of University of Turku, but as mentioned earlier in the previous chapter it would be good to have its own person inside of TRILA to handle the day-to-day security. This will help to make sure that all the little things that affect security will be handled correctly. Also this person can handle all the need to know access to different classified information. This is fixed by upgrading the current data protection group to also handle security aspects of TRILA.

T - 04 - Security guidance

T - 04 required that there are instructions on how classified information is being handled in the workplace. And while TRILA has these instructions they were not updated very regularly and not known to the employees. While writing this thesis I updated these instructions and informed everyone where they are found, so that they are easily available to everyone. By doing this it ensured that this section is done properly.

T - 05 - Resources for the security work

T - 05 required that following of the security guidelines are being managed, and that is done by University of Turku's security management. But as mentioned in the previous chapter it would be good that it is also managed inside of TRILA's day-to-day life, so this basically goes hand in hand with section T - 02 thus is also fixed by appointing a certain person or group to handle these security matters.

T - 11 - Non-disclosure and confidentiality commitment

T - 11 required that all personnel who handle classified information sign a non-disclosure agreement and this is handled how it should be done. But as mentioned previously it would clarify things a little bit more if all of the TRILA's employees would sign additional non-disclosure agreements on top of the already existing ones. This is not a necessary thing to do, but there is no harm in doing so. It would be more clear to clients if they knew that TRILA's personnel have their own non-disclosure agreement and not only the agreement that University of Turku requires.

T - 13 - Need-to-know and access rights

T - 13 required that the employees should only have access to classified information based on need to know. This is currently present in TRILA, but as mentioned previously it could be more clearer. While writing this thesis I have made up documentation where all the employees of TRILA are listed and all of the accesses each employee has. Also the need to know basis on those access. This will manage the need to know access rights, and especially when employees' contracts end, it will be easy to just check where that employee had access rights and then remove them.

I - 16 - Security throughout the information processing environment life cycle - change management

I - 16 required that all their security aspects are evaluated periodically which is done by the University of Turku's security management, but as mentioned in the previous chapter there also could be some kind of periodic evaluations inside of TRILA. This section also goes hand in hand with sections T - 02 and T - 05. When an employee is assigned to handle the security aspects inside of TRILA's day-to-day life this is one of the things that falls down to the employee.

6.2 Security Training

This section will include security training for TRILA's employees. Why it is needed and how it is conducted. There are also some examples of the teaching during this chapter to give better understanding of what the actual teaching exercises will be. The images from the actual training are in Finnish because the employees in TRILA speak Finnish.

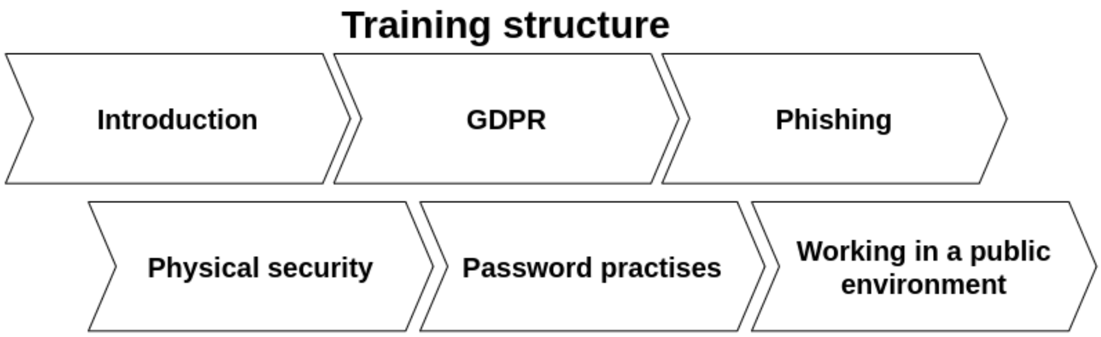


Figure 6.1: Training structure

As found in the research, TRILA's employees' information about security is not up to date. Therefore I am conducting a security training inside TRILA. This will be conducted by using ViLLE. Only purpose of this training is to get employees' security knowledge to the required level when handling personal information. The training will have a short section about GDPR, what it is and why it is important. Also some general information on how to handle data correctly and how to keep your physical security on required level.

Why is security training important? The main reason why security training is so important is that employees do not accidentally do something that compromises the security of an organisation or classified information. When employees do not have up to date knowledge on security or knowledge in the first place they are due to compromise the security even though they are not doing that on purpose. This is the first thing that is explained to the employees when they start the security training.

The second thing that is explained to the employees during the training is what is the General Data Protection Regulation (GDPR). It is a privacy and security law made in Europe. It is made to protect people's personal data and its rightful usage. For breaking this law organisations can be fined heavily [19]. What GDPR has to do with TRILA? TRILA collects and handles a lot of personal information, and these all are under the protection of GDPR. So when employees from TRILA is handling these said informations they have to know how to actually handle them without breaking the GDPR. After the brief introduction to what GDPR is and how to handle personal data correctly I made a few exercises for the employees to answer as an example figure 6.2 shows one of those GDPR related exercises.

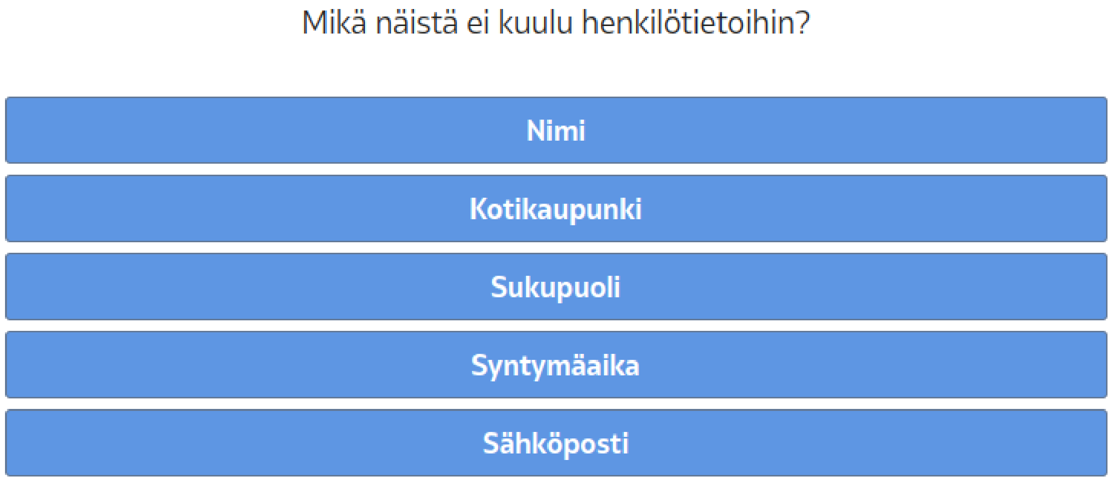
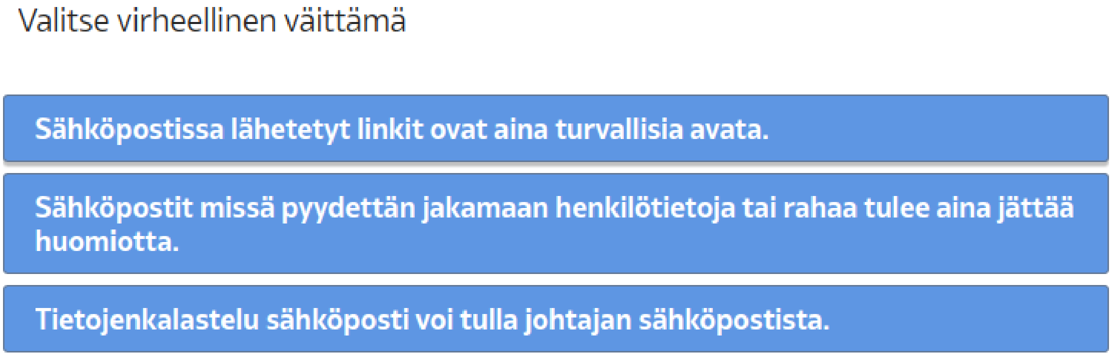

Mikä näistä ei kuulu henkilötietoihin?

Figure 6.2: Example image of GDPR exercise

Third chapter in the security training is about phishing. The purpose of phishing is to try to get the target to open an email link, which then can lead to some unwanted actions on the computer. Phishing is very common nowadays. It doesn't require much effort and can cause a great deal of damage. This is why it is very important to teach how to recognise phishing attempts. Usually phishing attempts can be recognised straight from the email that it was sent from, but there are cases when the email might come directly from your supervisor. This is why you can not open any links in email without knowing what it is. It is always good to keep in mind that there is no reason to share any personal information via email, especially your bank account information. Phishing is also becoming more and more a thing in cell phones. People are getting text messages where there are links, so the same rules apply there. Do not open these links, it is always better to ask an expert than trying it yourself. After employees have read through about phishing they have to answer one very simple exercise about phishing, which is seen in figure 6.3.



Valitse virheellinen väittämä

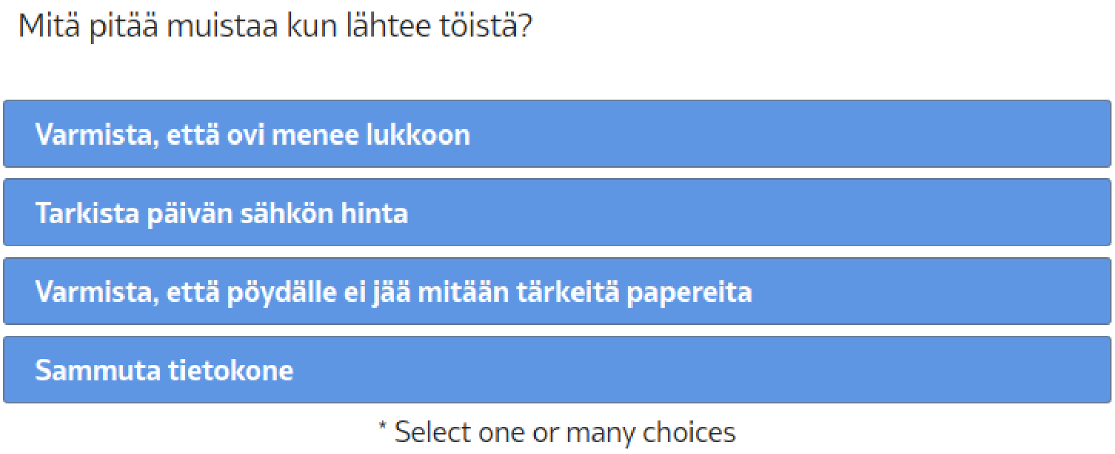
Sähköpostissa lähetetyt linkit ovat aina turvallisia avata.

Sähköpostit missä pyydettän jakamaan henkilötietoja tai rahaa tulee aina jättää huomiotta.

Tietojenkalastelu sähköposti voi tulla johtajan sähköpostista.

Figure 6.3: Example image of phishing exercise

After the phishing chapter the security training will approach physical security. Physical security is something that most people take for granted, when there are locks on the doors, but it is very important to remember that even though the doors are locked there is no need to leave your computer running when you are not using it. Also leaving some papers unsupervised is not a good practice. You should never leave anything work related unsupervised. Always make sure that you turn off your computer and lock the door when you leave. It is also worth mentioning that when working in public places you can not leave anything unsupervised, and you have to use a screen protector so people can not see what you are doing. As before I have made a simple exercise for employees to answer about physical security after they have read through the information about it, exercise can be seen in figure 6.4.



Mitä pitää muistaa kun lähtee töistä?

Varmista, että ovi menee lukkoon

Tarkista päivän sähkön hinta

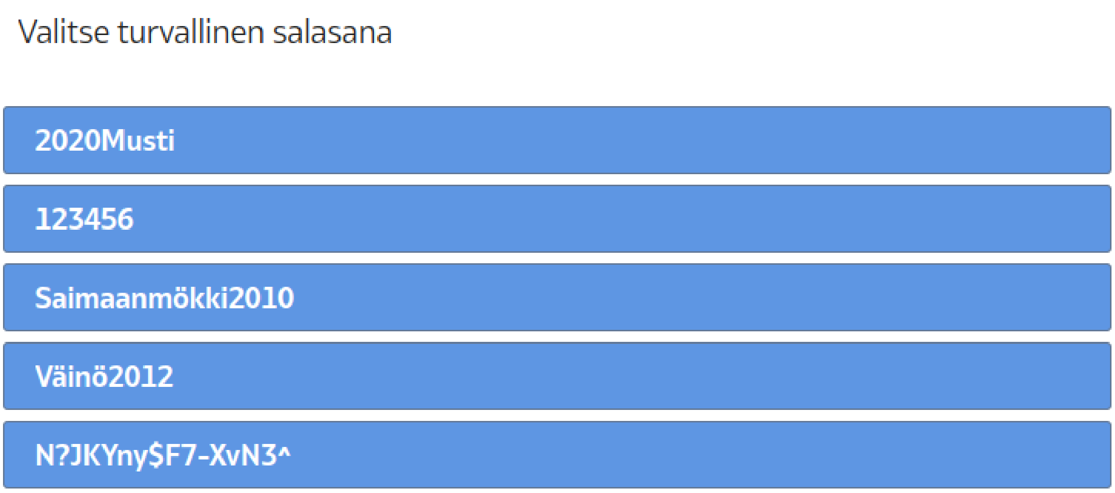
Varmista, että pöydälle ei jää mitään tärkeitä papereita

Sammuta tietokone

* Select one or many choices

Figure 6.4: Example image of physical security exercise

Fifth chapter in the security training is about good password practices. It is way too common that people use the same passwords pretty much in every account they own. You should only use one password per account, and because remembering is pretty much impossible you should use password management applications for example F-secures password manager. It stores your passwords safely and also generates complex enough passwords that they are safe. Passwords should have at least 16 characters and it should contain upper and lowercase letters, numbers and special characters. If your account contains classified information it should have a two factor authentication system on it. This will protect the account even more. I think it goes without saying that you should not share your password with anyone ever. Fifth chapter also holds the last exercise in this security training. I chose to keep the exercises very simple and they are there only to make sure that employees read through the information about the subjects in hand. The exercise about good password practices can be seen in figure 6.5.



Valitse turvallinen salasana

2020Musti

123456

Saimaanmökki2010

Väinö2012

N?JKYny$F7-XvN3^

Figure 6.5: Example image of password exercise

Last thing that I put in the security training was working from public places. This is becoming more and more popular so I figured it would be best to cover it as well. You should always use a protective layer on your screen so that bystanders cannot see what you are doing. Also when connecting to a public network VPN-services must be used. In TRILA's case University of Turku provides their own VPN-service. As I mentioned in the physical security section in this security training you should never leave your work related stuff unsupervised. Lastly if you are having a meeting in a public setting you should make sure that you are not discussing classified information, so that no one can overhear it by accident.

7 Summary

The pandemic gave digital learning a rather quick growth. It had been growing steadily over the last years, but the pandemic forced a lot of schools to change their style of teaching and to work with digital teaching. Because of this spike in users in digital learning platforms, security became more important than ever. This was one of the reasons I chose digital learning platforms and the way to improve their security as the main focus for this thesis. Doing the research I also created a new security evaluation method.

There were not any up-to-date security evaluation methods for digital learning platforms for my purposes, so in this thesis I chose to make a new one. The security evaluation method that was made was tested in a case-study. In this case-study the security of TRILA was also evaluated.

The case-study's results show that TRILA's security is in a rather good spot. There were few things that came up during the security evaluation that needed to be perfected, but nothing alarming. All of the improvements were shared with TRILA and implemented during this thesis.

The first thing that was discovered was that TRILA does not have a defined personnel of their own to handle the security aspects of the institute. Given that the current security personnel comes from the University of Turku's Digital Services, legally TRILA does not need to have a defined personnel inside their institute. All things aside it would be much easier and also safer for the institute to have someone to handle the security side of things. Before TRILA had a data protection group who handled all the GDPR related things. This group was upgraded to handle cyber security on top of data protection to help with the security side of things. There were also some improvements to the day-to-day life that fall upon the defined personnel, such as updating instructions regarding handling classified information and making sure that security guidelines are followed.

On top of that some improvements were made to ensure even safer data management. Extra non-disclosure agreements were made just for TRILA's employees who are handling classified information, even though there already is one from the University of Turku. Also the access rights were not clear enough, thus making it rather hard to manage. This was improved by making a document which includes all the access rights that each employee has. This is an easy way to manage the need to know access to certain information.

Lastly a security training was made for TRILA's employees. This will be held to all the new employees and also periodically to the old ones just to keep certain security aspects refreshed. The security training that was created is not very complex, it has the most common things that employees need to know and remember at all times.

The fact that even though TRILA has done everything rather securely, but still desperately needed security training for their employees is proof that this research is important. There are a lot of organisations that are doing everything by the book, but are forgetting the most important and the highest security risk there is, employees. Humans are the biggest security concern no matter what. Thus it is mandatory to organise security training periodically to employees.

What comes to the objectives of this thesis, those were fulfilled. Katakri was an excellent choice from which the evaluation method was built on. Security evaluation in my opinion was a success, there were things that were missing and needed some improvements but all of those were perfected. Thus making it definitely a positive thing for TRILA. What comes to the security training, I think it worked rather well. ViLLE was a perfect platform to make this kind of training for the employees to learn a little bit more about security.

Given the results from the case-study I can say that this method can be used in other learning ecosystems as well, to check and improve their security. It is important that in these learning ecosystems the security side is up-to-date because of how much personal information they are collecting and storing.

References

[1] Priyanka Sharma, Kirti Agarwal and Priya Chaudhary, "E-learning platform security issues and their prevention techniques: A review", in *International Journal Of Advance Scientific Research And Engineering Trends*, vol. 6, 2021, pp. 1–9.

[2] National Security Authority of Finland, "Katakri, Information Security Audit Tool for Authorities", in *Traficom publications*, vol. 232, 2020, pp. 1–116.

[3] Lance B. Coleman, *The ASQ Certified Quality Auditor Handbook*. ASQ Quality Press, 2020, ISBN: 9781951058111. [Online]. Available: `https://books.google.fi/books?id=VgmmEAAAQBAJ` (visited on 04/04/2023).

[4] Mauro Callejas-Cuervo, Andrea C. Alarcón-Aldana and Alexander L. Barinas, "Security evaluation model for virtual learning environments", in *2016 XI Latin American Conference on Learning Objects and Technology (LACLO)*, 2016, pp. 1–6.

[5] Umesh H. Rao and Umesha Nayak, *The InfoSec Handbook: An Introduction to Information Security*. Apress, 2014, ISBN: 9781430263838. [Online]. Available: `https://books.google.fi/books?id=Qe9lBAAAQBAJ` (visited on 04/04/2023).

[6] Meghna Bhatia and Dr. J. K. Maitra, "E-learning platforms security issues and vulnerability analysis", in *2018 International Conference on Computational*

and Characterization Techniques in Engineering Sciences (CCTES), 2018, pp. 276–285.

[7] Finnish Transport and Communications Agency, "Criteria to Assess the Information Security of Cloud Services (PiTuKri)", in *Traficom publications*, vol. 20, 2020, pp. 1–64.

[8] Google, *Google workspace.* [Online]. Available: `https://workspace.google.com/` (visited on 02/28/2023).

[9] Trello, *Trello website.* [Online]. Available: `https://trello.com/en` (visited on 02/28/2023).

[10] Slack, *Slack website.* [Online]. Available: `https://slack.com/` (visited on 02/28/2023).

[11] Microsoft, *Microsoft teams.* [Online]. Available: `https://www.microsoft.com/en-us/microsoft-teams/group-chat-software` (visited on 02/28/2023).

[12] Zoom, *Zoom website.* [Online]. Available: `https://zoom.us/` (visited on 02/28/2023).

[13] Github Inc, *Github website.* [Online]. Available: `https://github.com/about` (visited on 02/28/2023).

[14] Microsoft, *Microsoft exchange.* [Online]. Available: `https://www.microsoft.com/en-us/microsoft-365/exchange/email` (visited on 02/28/2023).

[15] Wordpress, *Wordpress website.* [Online]. Available: `https://wordpress.com/about/` (visited on 02/28/2023).

[16] YouTube, *Youtube website.* [Online]. Available: `https://about.youtube/` (visited on 02/28/2023).

[17] Echo360, *Echo360 website.* [Online]. Available: `https://echo360.com/` (visited on 02/28/2023).

[18] Seafile, *Seafile website*. [Online]. Available: `https://www.seafile.com/en/home/` (visited on 02/28/2023).

[19] Ben Wolford, *What is GDPR, the EU's new data protection law*. [Online]. Available: `https://gdpr.eu/what-is-gdpr/?cn-reloaded=1` (visited on 02/28/2023).

Appendix A Interview with Petra Enges about TRILA

1. What is the Turku Research Institute of Learning Analytics?

2. When and how everything started?

3. What is the main purpose of TRILA?

4. What are the biggest achievements of TRILA so far?

5. What is TRILA's impact on society?

Appendix B Interview with Juho about external services

1. What external services are used in TRILA?
2. What external services are we offering?
3. Why are we using them?
4. What are we using that service for?