Deployment and Management Tool of Security Areas

Tomi Makkonen

Master’s thesis
November 2024
Master's Degree Programme in Information Technology, Cyber Security

Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Description

Makkonen, Tomi

Deployment and Management Tool of Security Areas

Jyväskylä: Jamk University of Applied Sciences, November 2024, 68 pages.

Master's Degree Programme in Information Technology, Cyber Security. Master’s thesis.

Permission for open access publication: Yes

Language of publication: English

Abstract

The development of physical security is essential for safety-conscious authorities and public administrations in Finland, which have a statutory obligation to use the government security network (TUVE Act). The obligation to operate in such a network imposes more stringent requirements on the organisation's physical security. Various security frameworks, such as ISO 27001 and Katakri 2020, can be used to harden physical security. Katakri's security requirements can be used to audit and develop an organisation's security. The aim is to protect confidential information held by public authorities.

The purpose of this research was to develop an Excel-based tool for Helsinki City Rescue Services to deploy and manage security areas according to the Katakri 2020 requirements. Katakri 2020 recommends a risk-based approach to assessing safety requirements, so risk management processes were included in the tool. The research questions were what kind of risk assessment and management process would be suitable with the tool, how would the continuous improvement process work, and would the tool be suitable for other organisations that need to consider physical security.

The tool's physical security requirements, risk management, and continuous improvement processes were gathered through a literature review of known security frameworks such as ISO27001 and NIST, and other sources like governmental reports, scientific articles and journals. The first version of the tool was tested and evaluated by experienced security experts working in the governmental and public sector, and peer interviews were conducted with them.

Based on the interviews' results, the tool's risk assessment and management processes were found to be good as it was considered simple yet comprehensive. Risk assessment that is too complex is usually not carried out. It was also suggested that qualitative risk assessment is sufficient for risk assessment and that the risk assessment scale should be kept simple. Continuous improvement process was considered essential and overall, such a tool was seen as useful.

Keywords/tags (subjects)

Security areas, Physical security, Katakri 2020, Risk management, Rescue services

Miscellaneous (Confidential information)

-

Makkonen, Tomi

Deployment and Management Tool of Security Areas

Jyväskylä: Jamk Jyväskylän ammattikorkeakoulu, marraskuu 2024, 68 sivua.

Master's Degree Programme in Information Technology, Cyber Security. Ylempi AMK-opinnäytetyö.

Julkaisulupa avoimessa verkossa: Kyllä

Julkaisun kieli: englanti

Tiivistelmä

Fyysisen turvallisuuden kehittäminen on olennaista turvallisuustietoisille viranomaisille ja julkishallinnolle, joilla on lakisääteinen käyttövelvoite turvallisuusverkosta (Laki julkisen hallinnon turvallisuusverkkotoiminnasta). Velvollisuus toimia tällaisessa verkossa asettaa organisaation fyysiselle turvallisuudelle tiukempia vaatimuksia. Fyysisen turvallisuuden koventamiseen voidaan käyttää erilaisia tietoturvakehyksiä, kuten ISO 27001 ja Katakri 2020. Katakrin tietoturvavaatimuksia voidaan käyttää organisaation tietoturvan auditointiin sekä kehittämiseen, ja tavoitteena on suojata viranomaisten hallussa olevaa salassa pidettävää tietoa.

Tämän tutkimuksen tarkoituksena oli kehittää Excel-pohjainen työkalu Helsingin kaupungin pelastuslaitokselle Katakri 2020 -vaatimusten mukaisten turvallisuusalueiden käyttöönottoon ja hallintaan. Katakri 2020 suosittelee riskiperusteista lähestymistapaa turvallisuusvaatimusten arviointiin, joten työkaluun sisällytettiin riskienhallintaprosessit. Tutkimuskysymykset olivat, millainen riskienarviointi ja riskienhallinta toimisi työkalun kanssa, miten jatkuvan parantamisen prosessi toimisi ja soveltuisiko työkalu myös muille organisaatioille, joille fyysinen turvallisuus on tärkeää.

Työkalun fyysisen turvallisuuden vaatimukset, riskinhallinta ja jatkuvan parantamisen prosessit koottiin kirjallisuuskatsauksen avulla tunnetuista turvallisuuden viitekehyksistä, kuten ISO27001 ja NIST sekä muista lähteistä kuten valtion julkaisut, tieteelliset artikkelit ja lehdet. Työkalun ensimmäistä versiota testattiin ja arvioitiin kokeneilla turvallisuusasiantuntijoilla, jotka työskentelevät valtionhallinnossa ja julkisella sektorilla, ja heidän kanssaan tehtiin vertaishaastatteluja.

Haastattelujen perusteella työkalun riskienarviointi ja riskienhallinta prosessit todettiin hyväksi, koska niitä pidettiin yksinkertaisena, mutta kattavana. Liian monimutkaista riskinarviointia ei yleensä tehdä. Lisäksi esille tuotiin, että laadullinen riskienarviointi on riittävä ja että riskinarviointiasteikko olisi pidettävä yksinkertaisena. Jatkuvaa parantamisen prosessia pidettiin olennaisen tärkeänä, ja kokonaisuutena tällaista työkalua pidettiin hyödyllisenä.

Avainsanat

Turvallisuusalueet, Fyysinen turvallisuus, Katakri 2020, Riskienhallinta, Pelastustoimi

Muut tiedot (salassa pidettävät liitteet)

-

Contents

Figures

1 Introduction

The Helsinki City Rescue Service is undergoing a transitional phase as it moves towards implementing the government security network (TUVE). The objective is to improve the security and reliability of the ICT services and foster and ensure cooperation with other national public authorities already using security networks. Using security networks (TUVE) in rescue services is mandatory per the Law on public administration security network operations (Finlex, 2015).

Using of government security network will add more physical and technical security requirements for the organisation. Helsinki City Rescue Services is currently utilising the Helsinki City administrative network. Thus, physical security requirements have been different from those of government security network, albeit physical security is essential for the organisation even now (Finlex, 2015).

The Ministry of Finance regulates and governs Valtori, which provides security network services for public authorities in Finland. The government security network is subject to strict security requirements and administrative specifications set forth by the service provider and the Ministry of Finance. These administrative requirements are specified in the Law on public administration security network operations (Finlex, 2015).

Due to the regulations and hardened security requirements for implementing and using the government security network in Helsinki City rescue services, the organisation will need a new way of planning and implementing the security areas and continuous processes to manage risks and necessary security controls.

As a result, the organisation requires a comprehensive tool that can facilitate the planning, management, and control of security vulnerabilities in the security areas. This thesis aims to identify practical methodologies and processes for creating such a tool, which can, in addition, be utilised by other public authorities in Finland. Developing this tool for Helsinki City rescue services will enable the efficient deployment of the government security network (TUVE) at locations and sites and maintain Katakri's recommended physical security requirements.

1.1 Case Organisation

Helsinki City Rescue Services is responsible for providing essential public safety services, such as emergency and rescue services, risk management, and civil defence in everyday and emergency situations across the Helsinki Metropolitan Area. The rescue services operation is to arrange these services by legal obligation, and the organisation is under the national direction of the Ministry of the Interior Department for Rescue Services. The administration is under the Social Services, Health Care, and Rescue Services Division and that belongs to the Helsinki City organisation, as shown in Figure 1 (Helsinki City Rescue Services, 2024).

There are 12 rescue stations located in and around Helsinki. The largest one is situated in Kallio and is referred to as the central rescue station. Additionally, there are four sea stations that house rescue service ships for conducting sea rescue operations and dealing with oil spills (Helsinki City Rescue Services, 2022a).

The organisation's mission is to improve Helsinki City's safety by decreasing accidents. The mission's base foundation is the assessment of accident risks, which aims to lessen the impact of accidents. Based on the mission, the organisation's vision is to create the world's safest city (Helsinki City Rescue Services, 2022b).

At the Helsinki City Rescue Services, a good team spirit is considered an essential value that forms the foundation of all operative levels. This invaluable value enables employees to tackle everyday problems together. Other important values are the authenticity of the organisation, equality, and relevance of the work (Helsinki City Rescue Services, 2022b).

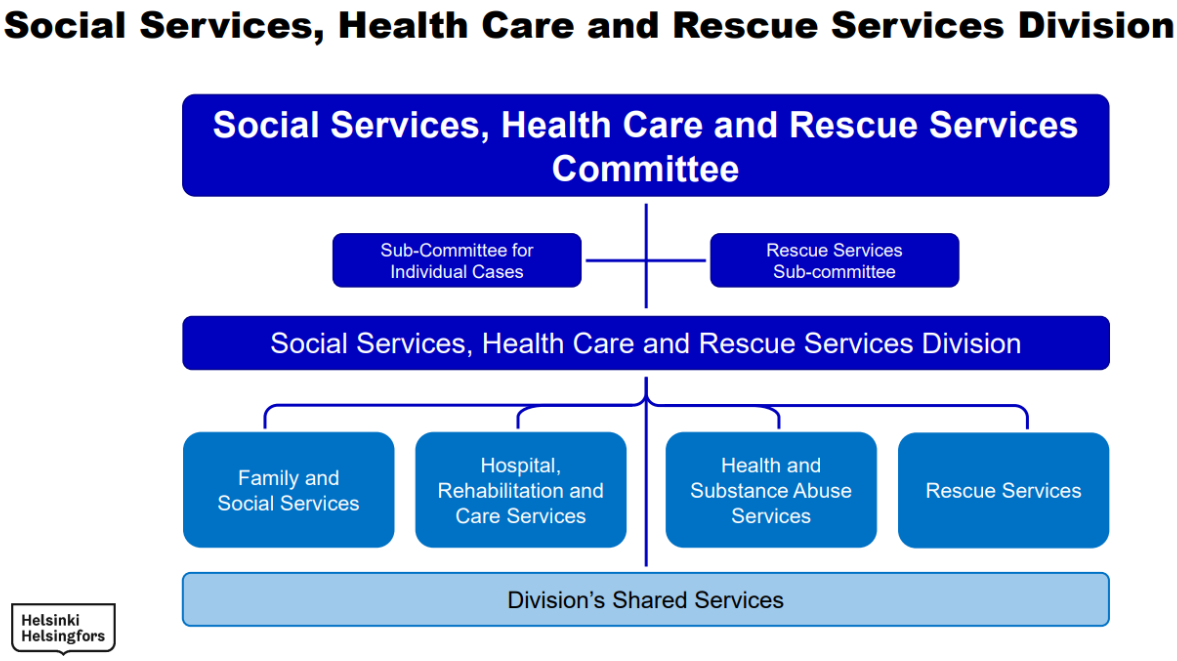

Social Services, Health Care and Rescue Services Division
Social Services, Health Care and Rescue Services Committee
Sub-Committee for Individual Cases
Rescue Services Sub-committee
Social Services, Health Care and Rescue Services Division
Family and Social Services
Hospital, Rehabilitation and Care Services
Health and Substance Abuse Services
Rescue Services
Division's Shared Services
Helsinki Helsingfors

Figure 1 Organisation 2024 (Organisation Chart, 2024).

1.2 Objectives and Research Method

The primary objective is to conduct research and develop an Excel-based tool for the organisation that will aid in the planning, definition, and management phases of administrative and security areas within the organisation based on Katakri 2020 requirements. It is worth noting that the tool will not cover technically secured areas. The tool's framework is based on the Law on public administration security network operations, Katakri's physical security requirements (NSA, 2020), scientific research articles, information, and physical security-related literature, and the ISO/IEC 27000 standard family (ISO/IEC 27000, 2022).

The secondary objective is to produce documentation for the case organisation on defined administrative and secured areas, outlining the risks involved and the physical security measures that should be implemented to mitigate them. These documents are classified and are not included in the appendices. Those documents can be shared with other rescue services, Helsinki City Health and Social Services, or Finland's public authorities when necessary.

The first version of the developed tool will have practical value for Helsinki City Rescue Services, and other rescue services can in addition use it. The tool's idea is to implement way to manage security areas more robust way, and all the related information can be found in the documentation created with the tool. It should in addition be helpful for other rescue services that are implementing and managing security areas and are requiring insights into what kind of security risks are related to the security areas and how to manage them with defence in depth methods and implemented physical security mechanisms.

The research questions are:

- What is a suitable risk assessment and management method, and how should it be implemented in the tool?
- How should a continuous management process be implemented within the tool?
- Is such a cross-functional tool, including risk management activities, useful for organisations that needs to consider physical security requirements and risks?

1.2.1 Chosen Research Method

The research method for this research and development project is based on qualitative research methods, including collecting theory from scientific articles, standards, and other related literature, and conducting interviews with experts in the field expertise.

The qualitative research method is employed when researching a phenomenon that cannot be explained with only data. This method is employed when trying to determine understandings for research questions such as "What does it mean?" and answering that needs theory background and a questionnaire related to the research questions. Qualitative research tries to determine answers to questions using words and phrases and not with numbers using statistical methods (Kananen, 2017).

The qualitative research method offers a new way to understand the phenomenon being studied. The focus is on research processes, which are hard to research using the quantitative research method because of their complexity. Collecting theory and analysing the results is solely based on the researcher. The researcher is interested in the processes and meanings of texts and photos (Kananen, 2017).

All the research questions focus on determining practical processes for the tool, how to implement them, and how they work with the tool. For that reason, a qualitative research method was chosen for this thesis because the research questions can be answered with a qualitative research method by gathering theories from security frameworks and relevant scientific articles and conducting interviews to measure the effectiveness of the implemented tool.

1.2.2 Related Research Projects

Throughout the literature review, it was determined that some research projects have similarities to this research. However, those theses focus was on improving general information security for rescue services, such as in information security practices for rescue departments (Kaipainen, 2015), which was developing ways to improve and maintain an organisation's information security. It is based on the older version of the Katakri and information classification. Another research was developing access control for the Länsi-Uusimaa Rescue Department (Harju, 2020) or security audit and development for the volunteer fire departments (Pukki, 2022). These were developing companies' information security or had some relations to Katakri and how to implement it for the companies' security. However, they were not developing a tool to deploy and manage secured areas' risks.

The related research project that most resembled this research was Minna Syri's development of a tool for improving an organisation's premises security (Syri, 2016). The focus of that research was to improve the case organisation's security by implementing a model for premises security, which is based on an older version of Katakri’s physical security requirements. That tool is based on the older Katakri’s version and does not include management of the risks and responsibilities of the area and the continuous management process.

1.2.3 Utility and Delimitation of This Research and Development Project

In contrast to prior research regarding similar topics, this thesis will research and implement a safety area management tool that has risk management processes implemented into it. By utilising the tool, the organisation can effectively deploy security areas by implementing assessment and management of the risks and continual improvement on the same tool, so all the needed information can be determined in one place, and management of those will be more straightforward. The practical application of this research will benefit the case organisation and other rescue services.

The research and development of the tool are based on the Katakri's (NSA, 2020) physical security requirements and ISO27000 standard family series (ISO/IEC 27000, 2022) physical security controls and processes. The focus is on the physical security section of Katakri 2020, but it will include some parts of the security management requirements. However, it's worth noting that the tool does not offer technical security control solutions or deployment and management of Katakri's technically secured areas.

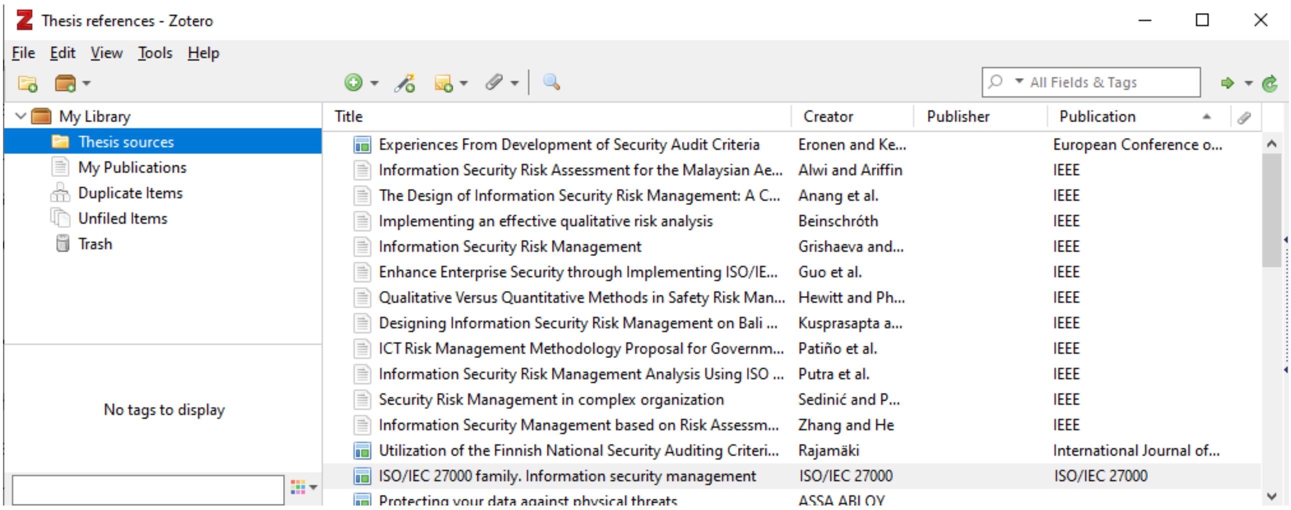
The tool will have a qualitative risk assessment method with a risk register and risk management processes implemented into it, and those processes are based on the Katakri 2020 and ISO27000 standard family series. The tool will utilise the Katakri 2020 defence in depth analytical approach to the risk assessment of the security areas. It will be a multi-purpose tool, and the safety area owner will use it to manage the security area with a continual management process. The tool is only meant to deploy and manage administrative and secured areas and is not meant to be employed to manage the physical security of the facility's outer perimeter or technically secured areas.

The finished tool will not be a new software; it is built with Microsoft Excel. It is only meant to improve the organisation's maturity level in managing security areas. Auditing should be done using the official Katakri 2020 auditing tool (NSA, 2020).

1.3 Framework of the Thesis

The thesis is structured into various sections, as shown in Figure 1. The initial segment is the introduction, serving as an overview of the thesis and fundamental details about the Helsinki City Rescue Services organisation, the thesis objective, related main questions, and the chosen research method.

The second segment contains the thesis's background theory. The theory was gathered from various databases and websites using several specific keywords. The sources were evaluated using the PRISMA Systematic Review, and non-relevant sources were excluded. Sources were managed using a Microsoft Excel sheet and the open-source reference management tool Zotero, as shown in Figure 2.



Title	Creator	Publisher	Publication
Experiences From Development of Security Audit Criteria	Eronen and Ke...		European Conference o...
Information Security Risk Assessment for the Malaysian Ae...	Alwi and Ariffin		IEEE
The Design of Information Security Risk Management: A C...	Anang et al.		IEEE
Implementing an effective qualitative risk analysis	Beinschróth		IEEE
Information Security Risk Management	Grishaeva and...		IEEE
Enhance Enterprise Security through Implementing ISO/IE...	Guo et al.		IEEE
Qualitative Versus Quantitative Methods in Safety Risk Man...	Hewitt and Ph...		IEEE
Designing Information Security Risk Management on Bali ...	Kusprasapta a...		IEEE
ICT Risk Management Methodology Proposal for Governm...	Patiño et al.		IEEE
Information Security Risk Management Analysis Using ISO ...	Putra et al.		IEEE
Security Risk Management in complex organization	Sedinić and P...		IEEE
Information Security Management based on Risk Assessm...	Zhang and He		IEEE
Utilization of the Finnish National Security Auditing Criteri...	Rajamäki		International Journal of...
ISO/IEC 27000 family. Information security management	ISO/IEC 27000		ISO/IEC 27000
Protecting your data against physical threats	ASSA ABLOY		

Figure 2 Open-source reference management tool Zotero.

The sources were identified via 8 databases and 33 websites, and the total number of identified relevant sources was 162. Relevant sources were pre-identified with specific keywords and the most frequent keywords employed for the databases and websites searches were information security, risk assessment, risk management, security management, PDCA, and Katakri. Non-relevant sources were already excluded during the pre-identification, so they were not part of the systematic review process.

The relevant sources were approved to be employed in the thesis by reviewing their abstracts and their relevance to the research questions, and the total number of approved sources was 114 and the number of excluded sources was 48. Based on the relevant sources' discussions and conclusions reviews, the number of chosen sources from the approved to be retrieved for the thesis was 50, as shown in Figure 3.

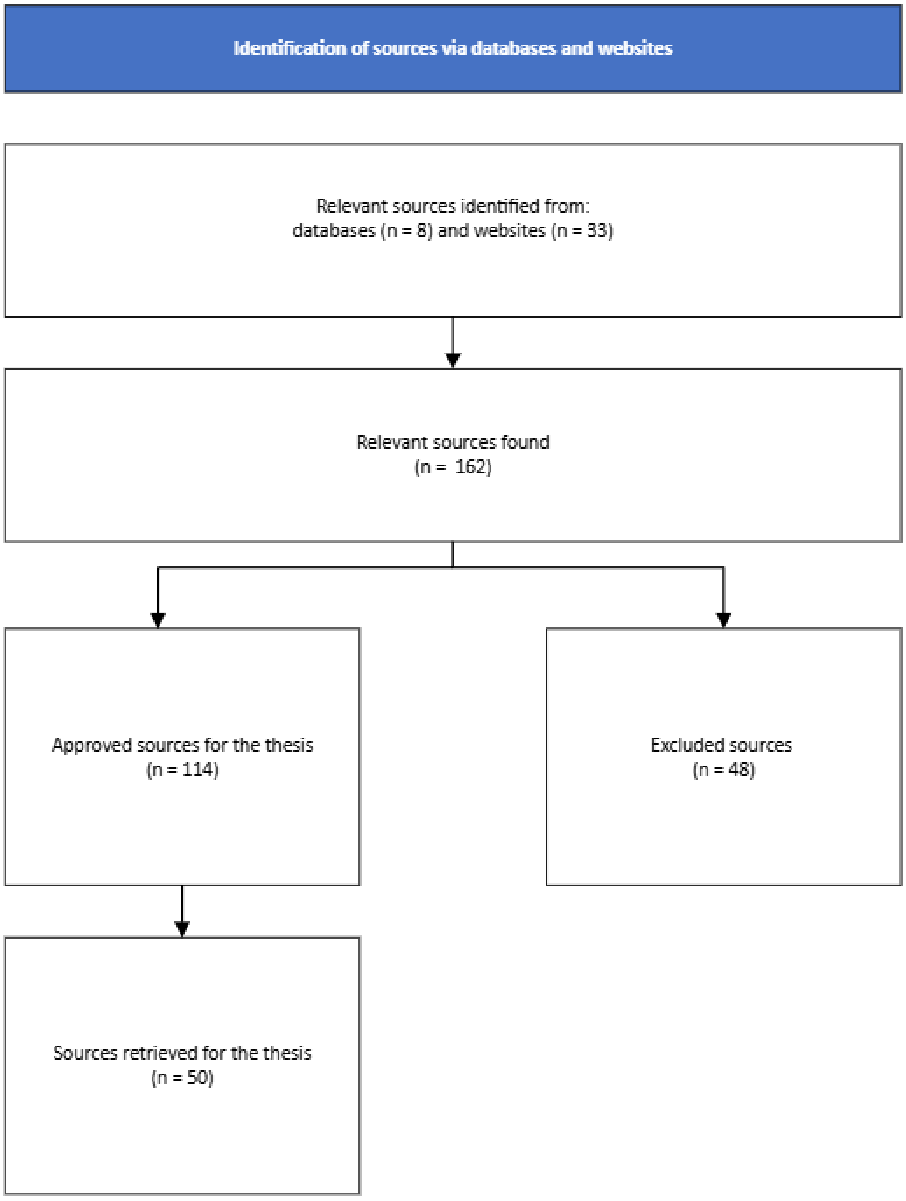

Identification of sources via databases and websites
Relevant sources identified from:
databases (n = 8) and websites (n = 33)
Relevant sources found
(n = 162)
Approved sources for the thesis
(n = 114)
Excluded sources
(n = 48)
Sources retrieved for the thesis
(n = 50)

Figure 3 PRISMA Flow Diagram.

The third and fourth segments are about the tool's implementation based on the gathered background theory as well anonymous peer interviews with security experts to evaluate its usability. Peer interviews were conducted October 2024 after finishing the first version of the tool. The target group of the interviews were specialists working in security and auditing field who had extensive experience in the related field. The final segment contains conclusions from the results of the peer interviews to address the research questions and discussions the potentials for further research, ethical values and how to get access for the tool.

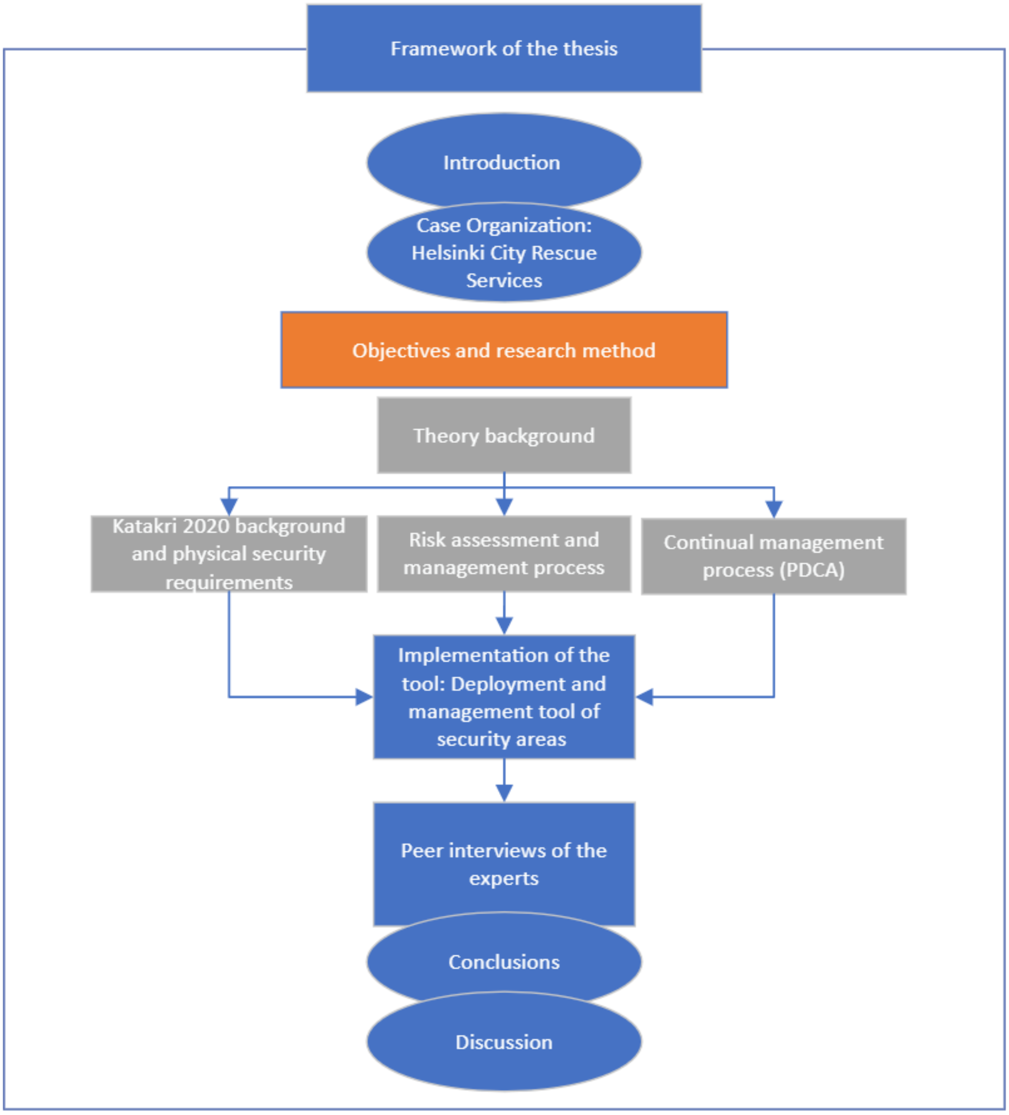

Framework of the thesis
Introduction
Case Organization: Helsinki City Rescue Services
Objectives and research method
Theory background
Katakri 2020 background and physical security requirements
Risk assessment and management process
Continual management process (PDCA)
Implementation of the tool: Deployment and management tool of security areas
Peer interviews of the experts
Conclusions
Discussion

Figure 4 Framework picture of the thesis.

2 Theory Knowledge for Developing the Tool

2.1 Katakri 2020

Katakri 2020 is a security auditing tool maintained by the National Security Authority of Finland and is employed by authorities. It has been part of the national security program since 2009 and was initially developed under the supervision of the Ministry of Defence. However, the responsibility for maintaining it was transferred to the NSA. The tool's latest version is the 2020 version and is designed to assist organisations in developing their security measures to protect classified information, and it includes three sections: security management, physical security, and information security (NSA, 2020; Cyberwatch Finland, 2021).

The Katakri 2020 has three sections: security management, physical security, and information security. These sections include minimum and recommended requirements for those three sections mentioned above. Security management has requirements for organisations on how to manage security and classified information and how to govern personnel security. The physical security section describes minimum requirements for the physical environment and how to protect the perimeter with different security mechanisms and standards. The information security section has requirements for the IT environment (NSA, 2020, p. 5; Cyberwatch Finland, 2021).

Katakri 2020 now includes an appendix for NATO's classification for security classification. National Security Authority approved the appendix as part of the Katakri 2020 on 4.4.2023. The appendix supports how to handle and store NATO's classified information. The NATO Office of Security has evaluated Katakri 2020 as a valuable tool for implementing and assessing security controls. Finland became a full member of NATO on the 4th of April 2023 (Finnish Government, 2023; NSA, 2023).

2.1.1 Security Areas

There are three levels of different security areas: administrative, secured, and technically secured. Finnish national legislation doesn't clarify technically secured areas, but it is included in Council of EU regulation. Administrative areas refer to normal office workspaces such as office rooms and meetings rooms, while secured areas are that where classified information is handled and stored. Technically secured areas are the highest security areas where internationally classified information is stored and handled. The zoning of security areas is based on the national decree of security classification of documents in the state administration. (Finlex, 2019; NSA, 2020, p. 22).

Prior to being approved for the chosen level, security areas must meet minimum security requirements. The implementation of physical security mechanisms and controls is based on the defence in depth method. This means that security should be evaluated through a risk assessment process as shown in Figure 5, and necessary security mechanisms and controls are based on the identified risks. Organisations should identify critical information and supportive business items and assets that require protection and choose appropriate layers of protection accordingly. The effectiveness of the selected security mechanisms and controls should be evaluated through continuous management. (NSA, 2020; Grishaeva & Borzov, 2021).

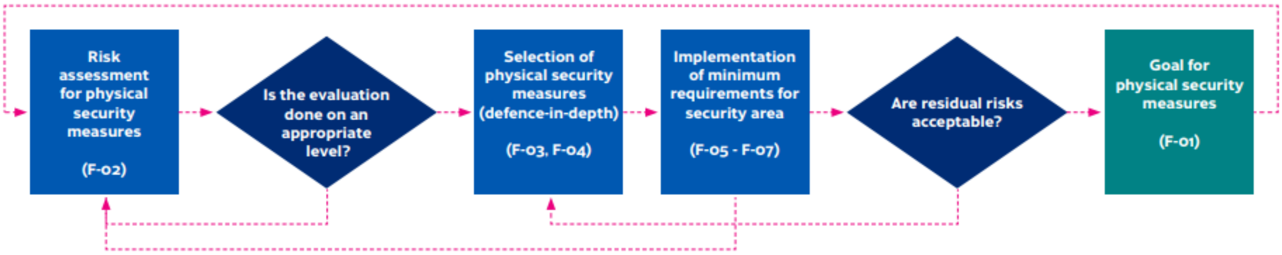
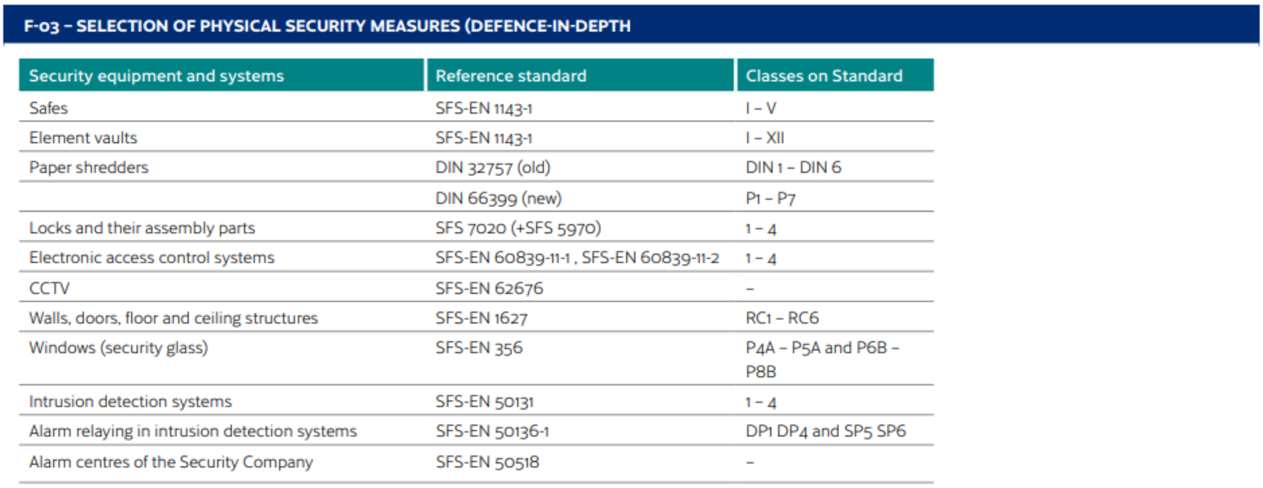

Risk assessment for physical security measures
(F-02)
Is the evaluation done on an appropriate level?
Selection of physical security measures (defence-in-depth)
(F-03, F-04)
Implementation of minimum requirements for security area
(F-05 - F-07)
Are residual risks acceptable?
Goal for physical security measures
(F-01)

Figure 5 Evaluation process for physical security measures (NSA, 2020, p. 23).

2.1.2 Physical Security

The purpose of physical security is to establish security measures and controls that prevent unauthorized access to classified information, theft or destruction of assets, and unauthorized entry into secured areas (ISO/IEC 27002, 2022; NSA 2020). One of the significant security controls is the implementation of national security clearances and clear access roles. Only personnel with assigned access roles and a national security clearance are allowed to enter secured areas, and the clearance level must match the sensitivity of the classified information they handle. In Finland, security clearance has three levels: concise, standard, and comprehensive (NSA, 2020, pp. 17-18; Finnish Security and Intelligence, 2024).

Required security mechanisms and devices are chosen with defence in depth method based on the risk assessment mentioned in Section 2.1.1. It is recommended that security mechanisms and devices be based on European standards and that they fulfil those requirements. Recommend standards for security mechanisms and devices are listed in Figure 6. Choosing the correct standard is additionally based on defence in depth method, so implementing them should be done most securely so that external users cannot access them. Security mechanisms include access control, camera surveillance, security staff, intrusion detection systems, physical controls such as security doors, area illumination, security staff, and security controls, including defined responsibilities and procedures (NSA, 2020, pp. 27-28).



F-03 – SELECTION OF PHYSICAL SECURITY MEASURES (DEFENCE-IN-DEPTH

Security equipment and systems	Reference standard	Classes on Standard
Safes	SFS-EN 1143-1	I – V
Element vaults	SFS-EN 1143-1	I – XII
Paper shredders	DIN 32757 (old)	DIN 1 – DIN 6
	DIN 66399 (new)	P1 – P7
Locks and their assembly parts	SFS 7020 (+SFS 5970)	1 – 4
Electronic access control systems	SFS-EN 60839-11-1 , SFS-EN 60839-11-2	1 – 4
CCTV	SFS-EN 62676	–
Walls, doors, floor and ceiling structures	SFS-EN 1627	RC1 – RC6
Windows (security glass)	SFS-EN 356	P4A – P5A and P6B – P8B
Intrusion detection systems	SFS-EN 50131	1 – 4
Alarm relaying in intrusion detection systems	SFS-EN 50136-1	DP1 DP4 and SP5 SP6
Alarm centres of the Security Company	SFS-EN 50518	–

Figure 6 Reference standards for security mechanisms and devices (NSA, 2020, p. 28).

2.2 Usability of Katakri and ISO27000 Standard Series for Organisations

Cross-case analysis (Rajamäki, 2015) discovered that documentation of security policies is helpful for companies, and they should define aspects such as long-term and short-term aims for security controls, indicators for those, and responsibilities and roles for security-related matters. More prominent organisations such as public administration or governmental organisations usually have personnel dedicated to security-related matters. Thus, they frequently direct those areas. Hence, those organisations have their documentation for security policies, but smaller organisations may be missing clear goals of security policies, or they are missing altogether (Rajamäki, 2015; Eronen & Kelo, 2020).

Katakri helps develop and audit security in an organisation because its security criteria and standards can be employed with different kinds of organisations, especially public administration, or governmental organisations. However, it does have its drawbacks, as those requirements and standards are not suitable for all organisations. Some requirements and standards allow interpretation instead of straightforward classification (Rajamäki, 2015; Eronen & Kelo, 2020).

Organisations have started using the ISO 27000 standard series to improve information security controls and assess and manage security risks. The standards are recognized by information security experts, and organisations can obtain information security certificates to prove their capabilities in information security. ISO 27002 has a comprehensive list of security controls, and ISO 27005 has risk assessment and management models for organisations. There are additionally other risk assessment methods with frameworks such as NIST 800-31, OCTAVE, or COBIT (Guo et al., 2022; Putra et al., 2020).

There are many ways to handle the security requirements and standards. Some organisations may want to minimise all the risks, and some try to determine an acceptable balance for the risks. Having several standards for a security criterion may create challenges. There are typically different views on how things should be protected, so it is recommended that security criteria have a clear use case, making the management process more accessible for users. The criterion may become useless when covering broader use cases (Eronen & Kelo, 2020).

2.3 Defining Security Areas

Defining security areas is crucial as it's a method to know what kind of classified information can be handled and stored in the defined security area or is there critical network devices, critical servers, other critical technical infrastructure, or other important assets. With the definition of the area the necessary security requirements, controls and standards can be chosen based on the evaluated risks (ISO/IEC 27002, 2022, Chapter 7. Physical controls; NSA, 2020, pp. 29-30).

One method to choose the security level of the area is according on what kind of handled and stored classified information is in the area, as shown in Figure 8 (Finnish) and Figure 9 (English). The English version of Katakri 2020 had errors on classification level descriptions that needed to be corrected on the time of writing this thesis, so the Finnish Figure 8 is employed as a cross-reference for the English Figure 9. National classified information should be principally stored and handled only in security areas. However, in some cases, classified information can be handled in public places, such as during remote work, which is considered out of the security areas (Finlex, 2019; NSA, 2020, pp. 29-30).

The second method evaluates the value of the organisation's most important assets and also areas that contains vital information or business-critical infrastructure which could damage or interfere with the organisation's operating environments in case that there are incidents. Security areas and their perimeters should be defined according to these requirements, and owner and role responsibilities for the secure area must be defined according to the requirements. ISO 27000 standard series framework can be employed with this method (ISO/IEC 27002, 2022, Chapter 7. Physical controls; Ross et al., 2020; ISO/IEC 22301, 2019).

Security areas must have clearly defined boundaries and be documented. It is recommended that they have floor plans with defined boundaries, as shown in Figure 7. The example shows how the organisation could document floor plans of the security areas. A variety of colours can be employed to separate area boundaries (Valtiovarainministeriö, 2013, p. 19-22).

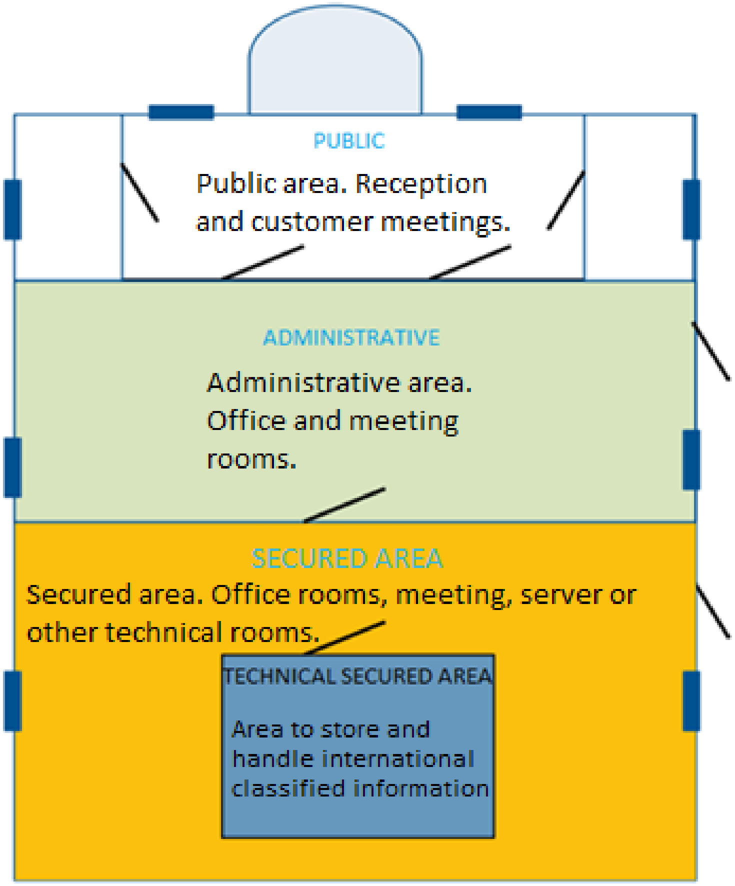
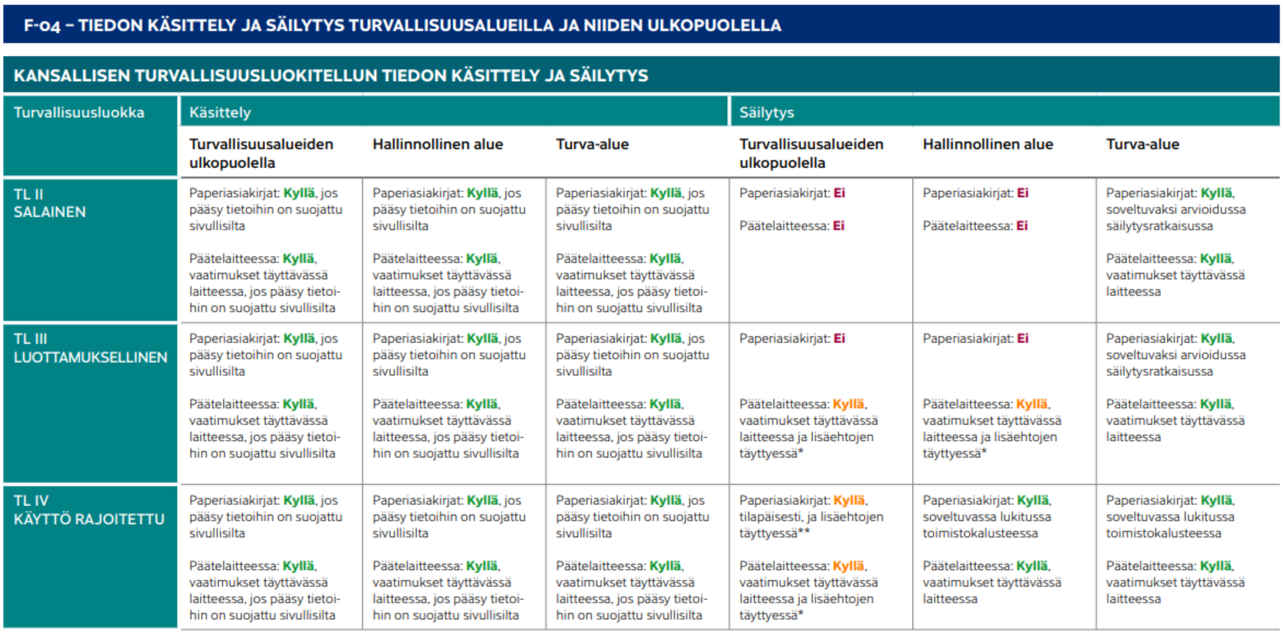

PUBLIC
Public area. Reception and customer meetings.
ADMINISTRATIVE
Administrative area. Office and meeting rooms.
SECURED AREA
Secured area. Office rooms, meeting, server or other technical rooms.
TECHNICAL SECURED AREA
Area to store and handle international classified information

Figure 7 An example of the security areas floor plans (Valtiovarainministeriö, 2013, p. 20).

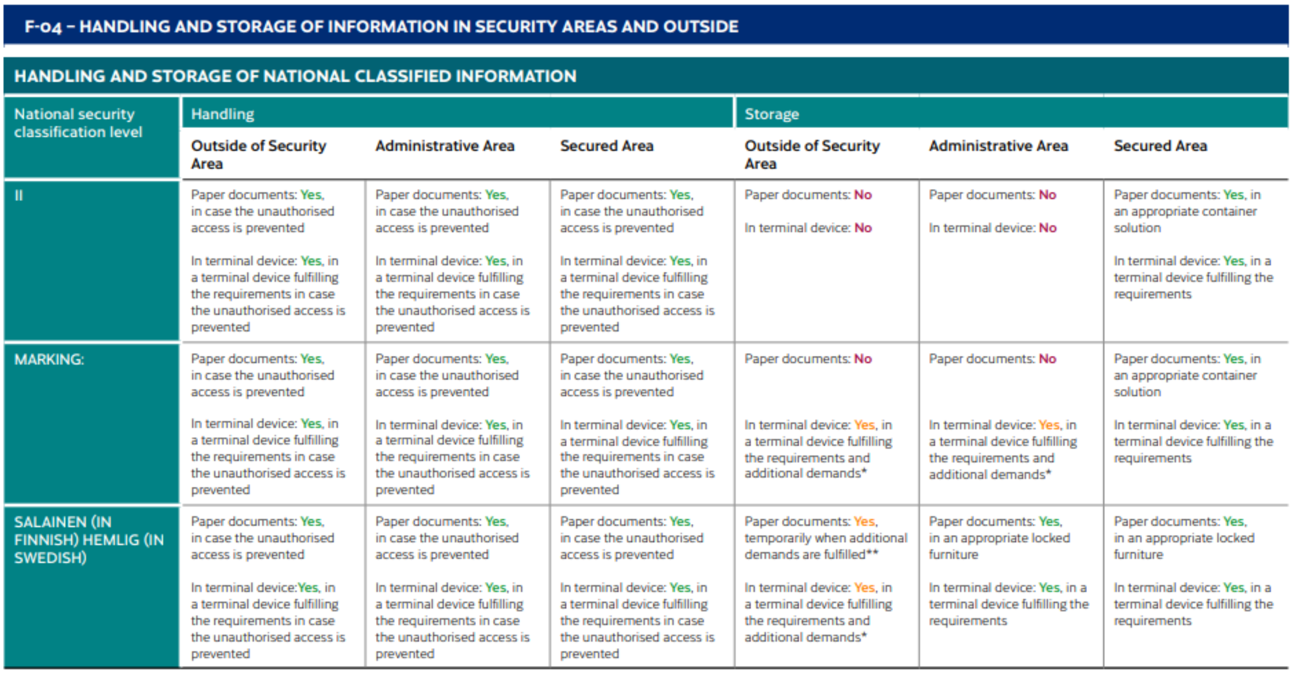


F-04 – TIEDON KÄSITTELY JA SÄILYTYS TURVALLISUUSALUEILLA JA NIIDEN ULKOPUOLELLA

KANSALLISEN TURVALLISUUSLUOKITELLUN TIEDON KÄSITTELY JA SÄILYTYS

Turvallisuusluokka	Käsittely			Säilytys		
	Turvallisuusalueiden ulkopuolella	**Hallinnollinen alue**	**Turva-alue**	**Turvallisuusalueiden ulkopuolella**	**Hallinnollinen alue**	**Turva-alue**
TL II SALAINEN	Paperiasiakirjat: **Kyllä**, jos pääsy tietoihin on suojattu sivullisilta Päätelaitteessa: **Kyllä**, vaatimukset täyttävässä laitteessa, jos pääsy tietoihin on suojattu sivullisilta	Paperiasiakirjat: **Kyllä**, jos pääsy tietoihin on suojattu sivullisilta Päätelaitteessa: **Kyllä**, vaatimukset täyttävässä laitteessa, jos pääsy tietoihin on suojattu sivullisilta	Paperiasiakirjat: **Kyllä**, jos pääsy tietoihin on suojattu sivullisilta Päätelaitteessa: **Kyllä**, vaatimukset täyttävässä laitteessa, jos pääsy tietoihin on suojattu sivullisilta	Paperiasiakirjat: **Ei** Päätelaitteessa: **Ei**	Paperiasiakirjat: **Ei** Päätelaitteessa: **Ei**	Paperiasiakirjat: **Kyllä**, soveltuvaksi arvioidussa säilytysratkaisussa Päätelaitteessa: **Kyllä**, vaatimukset täyttävässä laitteessa
TL III LUOTTAMUKSELLINEN	Paperiasiakirjat: **Kyllä**, jos pääsy tietoihin on suojattu sivullisilta Päätelaitteessa: **Kyllä**, vaatimukset täyttävässä laitteessa, jos pääsy tietoihin on suojattu sivullisilta	Paperiasiakirjat: **Kyllä**, jos pääsy tietoihin on suojattu sivullisilta Päätelaitteessa: **Kyllä**, vaatimukset täyttävässä laitteessa, jos pääsy tietoihin on suojattu sivullisilta	Paperiasiakirjat: **Kyllä**, jos pääsy tietoihin on suojattu sivullisilta Päätelaitteessa: **Kyllä**, vaatimukset täyttävässä laitteessa, jos pääsy tietoihin on suojattu sivullisilta	Paperiasiakirjat: **Ei** Päätelaitteessa: **Kyllä**, vaatimukset täyttävässä laitteessa ja lisäehtojen täyttyessä*	Paperiasiakirjat: **Ei** Päätelaitteessa: **Kyllä**, vaatimukset täyttävässä laitteessa ja lisäehtojen täyttyessä*	Paperiasiakirjat: **Kyllä**, soveltuvaksi arvioidussa säilytysratkaisussa Päätelaitteessa: **Kyllä**, vaatimukset täyttävässä laitteessa
TL IV KÄYTTÖ RAJOITETTU	Paperiasiakirjat: **Kyllä**, jos pääsy tietoihin on suojattu sivullisilta Päätelaitteessa: **Kyllä**, vaatimukset täyttävässä laitteessa, jos pääsy tietoihin on suojattu sivullisilta	Paperiasiakirjat: **Kyllä**, jos pääsy tietoihin on suojattu sivullisilta Päätelaitteessa: **Kyllä**, vaatimukset täyttävässä laitteessa, jos pääsy tietoihin on suojattu sivullisilta	Paperiasiakirjat: **Kyllä**, jos pääsy tietoihin on suojattu sivullisilta Päätelaitteessa: **Kyllä**, vaatimukset täyttävässä laitteessa, jos pääsy tietoihin on suojattu sivullisilta	Paperiasiakirjat: **Kyllä**, tilapäisesti, ja lisäehtojen täyttyessä** Päätelaitteessa: **Kyllä**, vaatimukset täyttävässä laitteessa ja lisäehtojen täyttyessä*	Paperiasiakirjat: **Kyllä**, soveltuvassa lukitussa toimistokalusteessa Päätelaitteessa: **Kyllä**, vaatimukset täyttävässä laitteessa	Paperiasiakirjat: **Kyllä**, soveltuvassa lukitussa toimistokalusteessa Päätelaitteessa: **Kyllä**, vaatimukset täyttävässä laitteessa

Figure 8 National security classification levels in Finnish (NSA,2020. p. 30).



F-04 – HANDLING AND STORAGE OF INFORMATION IN SECURITY AREAS AND OUTSIDE

HANDLING AND STORAGE OF NATIONAL CLASSIFIED INFORMATION

National security classification level	Handling			Storage		
	Outside of Security Area	**Administrative Area**	**Secured Area**	**Outside of Security Area**	**Administrative Area**	**Secured Area**
II	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	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: **No** In terminal device: **No**	Paper documents: **No** In terminal device: **No**	Paper documents: Yes, in an appropriate container solution In terminal device: Yes, in a terminal device fulfilling the requirements
MARKING:	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	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: **No** In terminal device: Yes, in a terminal device fulfilling the requirements and additional demands*	Paper documents: **No** In terminal device: Yes, in a terminal device fulfilling the requirements and additional demands*	Paper documents: Yes, in an appropriate container solution In terminal device: Yes, in a terminal device fulfilling the requirements
SALAINEN (IN FINNISH) HEMLIG (IN SWEDISH)	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	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, temporarily when additional demands are fulfilled** In terminal device: Yes, in a terminal device fulfilling the requirements and additional demands*	Paper documents: Yes, in an appropriate locked furniture In terminal device: Yes, in a terminal device fulfilling the requirements	Paper documents: Yes, in an appropriate locked furniture In terminal device: Yes, in a terminal device fulfilling the requirements

Figure 9 National security classification levels in English (NSA, 2020, p. 30).

2.4 Minium Physical Security Requirements of Administrative Areas

Administrative areas are regular office rooms, workspaces, or meeting rooms. The area must have a documented and defined boundary, and independent access is only provided to authorized personnel. Prior the area can be approved; it must be filled with the minimum required security mechanisms and controls. A risk assessment must be done for the area and plans for responsibilities and management for the risks must be made to accept residual risks (NSA, 2020, p. 33; NSA, 2020, pp. 25-27).

National classified information TL IV can be stored and handled in administrative areas, and it is recommended that the information is stored in office furniture, which can be locked. It is possible to store TL III information in an administrative area when the information is stored in hardened computers, which fills the requirements for storing TL III information, and these requirements can be found in Katakri 2020 I-section. However, the area must be protected with a burglar alarm system as explained under the heading of administrative area minimum requirements for security mechanism and controls, No. 5 security control. Computers must be additionally kept in a locked office furniture (NSA, 2020, p. 33; NSA, 2020, pp. 29-32; NSA, 2020, pp. 40-41).

Administrative area minimum requirements for security mechanisms and controls

No.	Security control / mechanisms	Brief description
1	Boundaries of the area and structures	Area must have documented and defined boundary. There are no requirements for structures or structural integrity (NSA, 2020, p. 33).

The boundaries of the area must be documented and defined. Area structures should be reinforced with necessary security mechanisms and recommended reference standards, as shown in Figure 6, provided that classified information is stored in the area and the probability of burglary exists. The area should have no open holes, all the walls and floor structures should be one solid structure, and the doors of the boundary must all the time be locked. If possible, emergency exits should not go through the area (ISO/IEC 27002, 2022, Chapter 7. Physical controls; NSA, 2020, p. 33).

No.	Security control / mechanisms	Brief description
2	Access management of the area	Only approved personnel may have independent access to area. Access rights and key management must have defined policies and roles (NSA, 2020, pp. 34-35).

Personnel must have organisation's approved security clearance to work independently in the area and wear visible identification card or equivalent. Access to the area can be security controlled mechanically or electrically, and access rights and keys management must have a named responsibility person. Access rights and keys must be documented, and management of the keys and rights must have a continual process, which includes updating, removing, and adding access rights and keys. All the access rights events must be logged. Backup keys for the area must be stored safely, such as in access-controlled key cabinets or similar solutions. (ISO/IEC 27002, 2022, Chapter 7. Physical controls; NSA, 2020p, pp. 34-35).

No.	Security control / mechanisms	Brief description
3	Visitors and third-party suppliers' management	Visitors must always be accompanied by a host, who must have permission to work independently in the area (NSA, 2020, p. 36).

Visitors must be identified by a visitor ID or equivalent and escorted within the administrative area by a host with independent access. Third-party maintenance and cleaners should only have access to necessary areas. Third-party supplier' personnel access rights can only be approved by the area's owner and access management responsibility person (ISO/IEC 27002, 2022, Chapter 7. Physical controls; NSA, 2020, p. 36).

Visitors must wear provided visitor identification by the organisation, and the details of the visit purpose must be logged, including the dates and times of check-in and check-out. Organisation personnel must have introductions on how to control visitors and their visits. Host must ensure that visitors cannot see, read, or hear the classified information (ISO/IEC 27002, 2022, Chapter 7. Physical controls; NSA, 2020, p. 36).

No.	Security control / mechanisms	Brief description
4	Soundproofing of the area	Soundproofing of the area must be good enough to be prevent classified information conversations for falling in wrong hands. Risk-based approach is recommended (NSA, 2020, p. 37).

Office rooms must have security measures for classified information conversations, so soundproofing must be considered based on risk assessment in the room where those kinds of discussions are held. Risk assessment can be done by listening outside the room to determine how the conversations can be heard outside the area. At a minimum, the doors and windows must be closed when that kind of discussion happens in the area (ISO/IEC 27002, 2022, Chapter 7. Physical controls; NSA, 2020, p. 37).

Personnel participating in the discussion of classified information must be informed about what kind of classified information will be discussed and what the security level of information is. Need-to-know must be considered, and the personnel must have the necessary security clearance for participating in the discussions (ISO/IEC 27002, 2022, Chapter 7. Physical controls; NSA, 2020, p. 37).

No.	Security control / mechanisms	Brief description
5	Intrusion detection system	There are no requirements for administrative areas. IDS can be considered with risk-based approach (NSA, 2020, p. 38).

Burglar alarms can be installed on doors and windows in areas where classified information is stored, and the risk of burglary is assessed to be high. The recommendation is to install a burglar alarm when no one works 24 hours in the area, and classified information is stored there. It is in addition recommended that the burglar alarm systems are by European standards, as shown in Figure 6, and they must be tested occasionally and be fail-safe so they will work during blackout. Various burglar alarms exist, such as contact-based, motion sensors, and sound sensors. The correct system can be chosen with risk-based approach (ISO/IEC 27002, 2022, Chapter 7. Physical controls; NSA, 2020, p. 38).

No.	Security control / mechanisms	Brief description
6	Illicit observation	Illicit observation with intent or by mistake must be prevented with necessary security controls (NSA, 2020, p. 39).

Controls to reduce the risk of illicit observation include installing privacy screens in the area, or by using blinds or curtains for windows, or using security films on computer monitors. Classified information must be removed from whiteboards and other presentation devices when no longer needed. (ISO/IEC 27002, 2022, Chapter 7. Physical controls; NSA, 2020, p. 39).

No.	Security control / mechanisms	Brief description
7	Camera surveillance	Camera surveillance must be utilised to monitor perimeter of the facility (ISO/IEC 27002, 2022, Chapter 7. Physical controls; Ross et al., 2020, p. 32; NSA, 2020, p. 27).

The perimeter of the facility and access ways to the facility must be monitored with camera surveillance to protect the organisation's property and assets. Cameras should be deployed based on the risk assessment. Security personnel can utilise a live feed to monitor the area. Camera surveillance should meet European standards, as shown in Figure 6 (ISO/IEC 27002, 2022, Chapter 7. Physical controls; Ross et al., 2020, p. 32; NSA, 2020, p. 27).

Camera surveillance should be planned and deployed as stated in the K-method of Finance Finland’s guidance (Finance Finland, 2017). Requirements for the minimum time to keep the camera surveillance recordings should be planned with risk assessment, but the recommended minimum time to keep recordings should be at least one month (NSA, 2020, p. 45; Finance Finland, 2017).

No.	Security control / mechanisms	Brief description
8	Storing and handling information	National classified information TL IV can be stored in administrative area. All information must be stored in appropriate office furniture (NSA, 2020, pp. 40-41).

Administrative area must have an appropriate lockable office furniture to store national classified information (TL IV). Devices containing classified information (TL IV) must be also stored in suitable office furniture. Organisation can consider storing devices containing classified information (TL III) in administrative area, however then the area must implement intrusion detection system or have the area staffed all the time, as mentioned in administrative area security control number 5 (NSA, 2020, pp. 40-41).

Only personnel authorised to handle classified information stored in the area should have keys or access codes to office furniture where classified information is stored. Access codes and privileges should be changed whenever there is a change of personnel or there has been maintenance on the locks or there is suspect that the information has been compromised (NSA, 2020, pp. 40-41).

2.5 Minium Physical Security Requirements of Secured Areas

Secured areas are office rooms, meetings rooms and server rooms or other technical rooms, which are protected with better security controls than administrative area to allow handling and storing higher level national classified information in the area. Area must have documented and defined boundary and independent access is only provided to authorized personnel. Minimum required security mechanism and controls must be filled before the area can be approved. Risk assessment must be done for the area and plan responsibilities and management for the risks, so that the residual risks can be accepted (NSA, 2020, p. 42; NSA, 2020, pp. 25-27).

National classified information TL IV – II can be handled and stored in the secured area based on risk assessment and chosen security mechanisms. TL III information must be stored in lockable storage solutions, which are evaluated to be sufficient for storing them. TL III computers must be stored in lockable storage solutions in the area. If there is no suitable storage solution then the area walls, floors and ceilings must fill the requirements for the TL III by European standards, as shown in Figure 3 (NSA, 2020, p. 42; NSA, 2020, pp. 29-32; NSA, 2020, pp. 54-55).

Secured area minimum requirements for security mechanisms and controls

No.	Security control / mechanisms	Brief description
1	Boundaries of area and structures	Area must have defined boundaries. Walls, ceilings, floors, windows, and doors must be reinforced if there is no sufficient lockable storage solution (NSA, 2020, pp. 42-43).

The boundaries of the area must be documented and defined. Secured areas should be planned and deployed so that random personnel don't gain access to them. The area structure must be reinforced to fulfil the SFS-EN-1627 class RC3 standard requirements and necessary security mechanisms if there is no sufficient lockable storage solution. The area must have a burglar alarm system if the area is not staffed 24/7 or there are no regular inspections after working hours. (ISO/IEC 27002, 2022, Chapter 7. Physical controls; NSA, 2020, pp. 42-43).

Personnel working in the secure area must know the boundaries of the secured area, the security measures when working in the area and working in the area must be on a need-to-know basis. The area should have no open holes, all the walls and floor structures should be one solid structure, and the doors of the boundaries must all the time be locked. There should be no easily breakable spots in the area. Emergency exits cannot go through this area, but if there is need for a mandatory exception, the emergency exit must have a burglar alarm installed. A secured area cannot be accepted in case that an emergency exit goes through it and there is no sufficient lockable storage solution for the classified information in the area (ISO/IEC 27002, 2022, Chapter 7. Physical controls; NSA, 2020, pp. 42-43).

No.	Security control / mechanisms	Brief description
2	Access management of the area	Access to the area must be controlled with in-out controls or personally identifying personnel (ISO/IEC 27002, 2022, Chapter 7. Physical controls; NSA, 2020, pp. 44-47). Only approved personnel may have independent access to area. Access rights and key management must have defined policies and roles (NSA, 2020, pp. 44-47).

Access control can be implemented electrically or personally identifying personnel methods. Electrical access control should implement European standards, as shown in Figure 6. It is recommended to use two-way access control for in-out security control. Passageways to the secured area or technical rooms should have cameras to improve in-out security. Approved personnel must have organisation’s approved security clearance to work independently in the area and they must wear visible identification. The secured area must have a responsible person who must have a security clearance, and that person can grant independent access rights to the area (ISO/IEC 27002, 2022, Chapter 7. Physical controls; NSA, 2020, pp. 44-47).

Access rights and key management must have management processes and documentation, and access rights to the area must follow a need-to-know basis. Granting access rights should be based principle of least privilege when defining access to the secured area. Access management must have a continual process so that access rights must be regularly checked at least every six months. Backup keys to the secured area must be kept inside access-controlled locked key storage or similar solution (ISO/IEC 27002, 2022, Chapter 7. Physical controls; Ross et al., 2020, p. 12; NSA, 2020, pp. 44-47).

No.	Security control / mechanisms	Brief description
3	Visitors and third-party suppliers' management	Visitors must be all the time escorted by a host, who is approved by organisation to work independently in the area (NSA, 2020, p. 48).

Visitors must be identified by a visitor identification or equivalent and escorted by a host who has independent access to the secure area. All visits or maintenance works must be logged. Visitors must have special permission to access the area, and their reliability must be verified, or a confidentiality agreement must be made with them when visiting a secured area where classified information is handled and stored (ISO/IEC 27002, 2022, Chapter 7. Physical controls; NSA, 2020, p. 48).

The 3rd party suppliers and maintenance personnel must be monitored under the surveillance of person with independent access to the area. Visitors must all the time be under monitoring and be supervised. In exceptional cases, visitors whom the responsible person approves in the area can be cleared to be unescorted visitors. It should be done according to the access control management.

Cleaning and maintenance work is prohibited when handling classified information in secured areas. (ISO/IEC 27002, 2022, Chapter 7. Physical controls; NSA, 2020, p. 48).

No.	Security control / mechanisms	Brief description
4	Security guidance documentation	All secured areas must have security guidance documentation on how to store and handle classified information (NSA, 2020, p. 49).

Secured areas must have security guidance documentation on how to handle and store classified information and visitor and access management controls. Documentation should in addition include what security controls and mechanisms should be employed in the area (NSA, 2020, p. 49).

No.	Security control / mechanisms	Brief description
5	Soundproofing of area	Soundproofing of the area must prevent classified information conversations for falling in wrong hands (NSA, 2020, p. 50).

Secured areas must have soundproofing in case that classified information is discussed in the area, and there is a risk that the information can be heard outside the secured area. Personnel must ensure that windows and doors are closed when discussing classified information. The secured area has the same security requirements as the administrative area, so those security requirements and mechanisms and their standards should be filled in the secured area based on the risk assessment. (ISO/IEC 27002, 2022, Chapter 7. Physical controls; NSA, 2020, p. 50).

No.	Security control / mechanisms	Description
6	Intrusion detection system	Secured area which is not 24/7 staffed must be inspected on regular basis after working hours or the area must have burglar alarm system (NSA, 2020, p. 51).

Secured area doors and windows should have a burglary alarm system installed when the area is not staffed 24/7 or regular inspections after work cannot be conducted. The burglary alarm system must meet European standards, as shown in Figure 6. The alarm can be equipped with contact sensors, motion sensors, or sound sensors. This should be done with a risk assessment considering the secured area structures and the probability of burglary in the secured area, but at least it's important to have a burglary alarm system on the first-floor windows and doors (ISO/IEC 27002, 2022; NSA, 2020, pp. 51-52).

The organisation should administer the burglary alarm system, but it can be outsourced with risk assessment. The alarm can in addition be transferred to the security company, but the transfer should be monitored and duplicated. Inspection of the secured area outside working hours can be outsourced to a third-party security company, but the security company's staff must be educated on how to operate in the secured area (NSA, 2020, pp. 51-52).

No.	Security control / mechanisms	Description
7	Illicit observation	Illicit observation with intent or by mistake must be prevented with necessary controls. (NSA, 2020, p. 53).

The secured area has the same controls as the administrative areas, and illicit observation of the classified information must be prevented with the necessary controls listed in the minimum requirements for administrative section 2.3 (ISO/IEC 27002, 2022, Chapter 7. Physical controls; NSA, 2020, p. 53).

No.	Security control / mechanisms	Description
8	Camera surveillance	Camera surveillance should be employed in the passageways to the secured or inside the secured area (ISO/IEC 27002, 2022, Chapter 7. Physical controls; Ross et al., 2020, p. 32; NSA, 2020, p. 27).

The perimeter of the secured areas should be monitored with camera surveillance. Camera surveillance must be employed in the passageways to the secured or inside the secured area to monitor and manage security incidents of the area and increase security methods to have increased controls with in-out access. Security personnel can use live feed to monitor the area. Camera surveillance should meet European standards, as shown in Figure 6, and should be planned and deployed using the K-method as stated in Finance Finland's guidance (ISO/IEC 27002, 2022, Chapter 7. Physical controls; Ross et al., 2020, p. 32; NSA, 2020, p. 27; Finance Finland, 2017).

No.	Security control / mechanisms	Brief description
9	Storing and handling information	Nationally classified information TLIV and TLIII can be stored in this area based on a risk assessment, considering that the area has a suitable storage solution (NSA, 2020, pp. 54-55).

Nationally classified information TLIV and TLIII can be stored in this area based on a risk assessment, considering that the area has a suitable storage solution. In case that the storage solution is inadequate, it must be ensured that the structures in the area have the required level of safety (NSA, 2020, pp. 54-55).

Only personnel authorised to handle classified information stored in the area should have keys or access codes to office furniture where classified information is stored. Access codes and privileges should be changed whenever there is a change of personnel or there has been maintenance on the locks or there is suspect that the information has been compromised (NSA, 2020, pp. 54-55).

No.	Security control / mechanisms	Brief description
10	Handling TLII information in the area	All electrical equipment must be inspected before handling TLII classified information in the secured area. Electrical equipment may be left outside the security area within the proper storage solution if it cannot be reliably inspected. (NSA, 2020, p. 53).

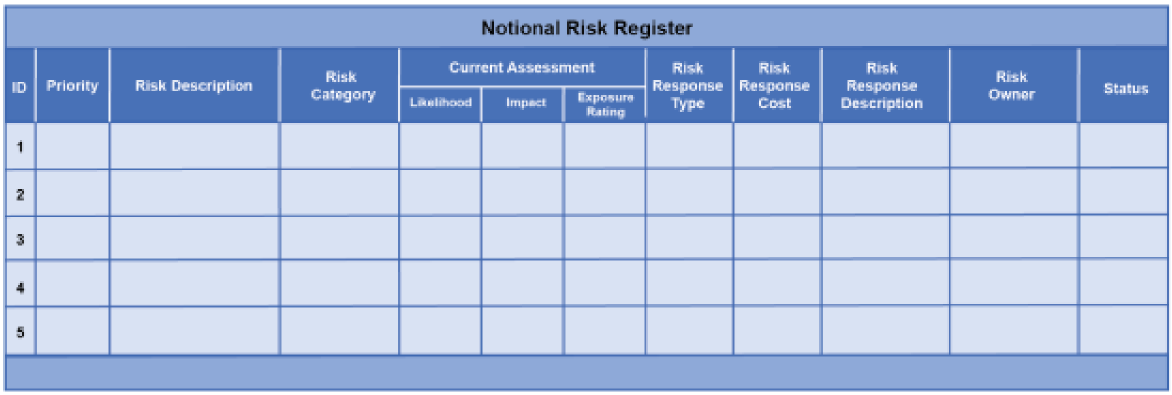
Temporary handling of TLII classified information in a secure area is possible, but all electrical equipment must be checked in case that there is a high risk of handling the classified information. Whenever inspecting the electrical devices reliably is not possible, the devices can be stored outside the security area inside a proper storage solution (NSA, 2020, p. 53).

2.6 Risk Assessment Process

The purpose of the risk assessment is to understand what kind of threats may affect organisation's assets and information and on how to evaluate and manage them. Organisation must recognise the important assets and information and evaluate their value or business criticality. There are various methods to do risk assessment, and two of the most central are qualitative and quantitative methods. Quantitative methods need more expertise and database of inputs from longer period as told in ISO 27005 standard (ISO/IEC 27005) and research conducted by Beinschróth (Beinschróth, 2022). Quantitative method for risk analysis is found quite frequently expensive and it's frequently conducted by large consulting firms, who has data for that kind of assessment (Beinschróth, 2022; ISO/IEC 27005, 2022, Annex A. Examples of techniques in support of the risk assessment process).

Qualitative method for risk assessment can be done easily by the organisation itself and it doesn't need many resources or time invest from the organisation, but it doesn't all the time give exact results and occasionally they have been discovered unusable by IT security experts. Qualitative method has its limitations when it comes to risk assessment, but it can in addition provide quick overview of the risks affecting the organisation's assets without the need of collecting extensive data and process them, which can be a lengthy process and need more resources and time investment. Carefully planning qualitative risk assessment with real effort and teamwork, documentation, and determining specific threats affecting organisation will reduce the risk of having an unusable risk assessment with qualitative method (Hewitt & Pham, 2018; Beinschróth, 2022).

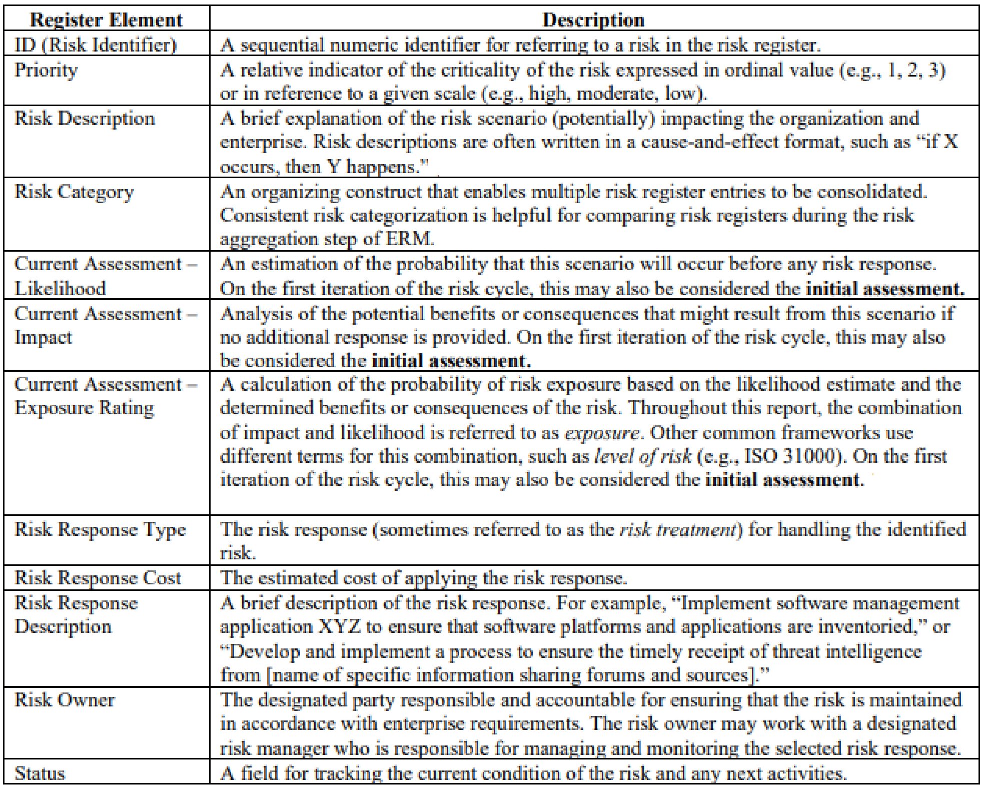
Organisations should have risk management process or framework and with that the organisation should have risk registers which contains information about risks, which can affect the organisation's assets or information. Risk management process can be based on ISO 27005 risk management process and most common tools to handle risks are using risk register. Risk registers should include risk identification, probability and likelihood of the risk, risk level, impact of the risk on the asset, recommended risk treatment or controls to reduce the level of the risk and the owner of the risk, as well responsible person for accepting the residue risk. Example of the risk register is shown in Figure 10 and descriptions explained in Figure 11. The risk register must have a continuous management, which must be checked for minimum at least half a year, so that residual risks are assessed with the risk owner (Sedinić & Perušić, 2015; Zhang & He, 2021).



Notional Risk Register

ID	Priority	Risk Description	Risk Category	Current Assessment			Risk Response Type	Risk Response Cost	Risk Response Description	Risk Owner	Status
				Likelihood	Impact	Exposure Rating					
1											
2											
3											
4											
5											

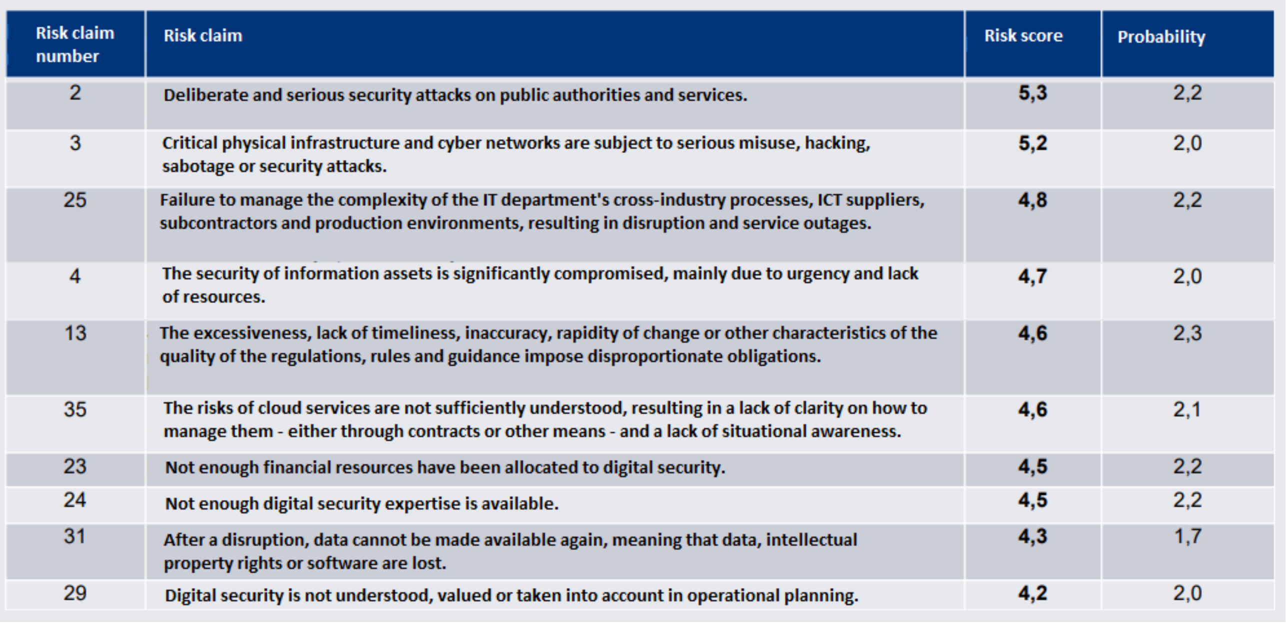
Figure 10 Example of risk register (Quinn et al., 2023, p. 26).



Register Element	Description
ID (Risk Identifier)	A sequential numeric identifier for referring to a risk in the risk register.
Priority	A relative indicator of the criticality of the risk expressed in ordinal value (e.g., 1, 2, 3) or in reference to a given scale (e.g., high, moderate, low).
Risk Description	A brief explanation of the risk scenario (potentially) impacting the organization and enterprise. Risk descriptions are often written in a cause-and-effect format, such as "if X occurs, then Y happens."
Risk Category	An organizing construct that enables multiple risk register entries to be consolidated. Consistent risk categorization is helpful for comparing risk registers during the risk aggregation step of ERM.
Current Assessment – Likelihood	An estimation of the probability that this scenario will occur before any risk response. On the first iteration of the risk cycle, this may also be considered the **initial assessment.**
Current Assessment – Impact	Analysis of the potential benefits or consequences that might result from this scenario if no additional response is provided. On the first iteration of the risk cycle, this may also be considered the **initial assessment.**
Current Assessment – Exposure Rating	A calculation of the probability of risk exposure based on the likelihood estimate and the determined benefits or consequences of the risk. Throughout this report, the combination of impact and likelihood is referred to as *exposure*. Other common frameworks use different terms for this combination, such as *level of risk* (e.g., ISO 31000). On the first iteration of the risk cycle, this may also be considered the **initial assessment**.
Risk Response Type	The risk response (sometimes referred to as the *risk treatment*) for handling the identified risk.
Risk Response Cost	The estimated cost of applying the risk response.
Risk Response Description	A brief description of the risk response. For example, "Implement software management application XYZ to ensure that software platforms and applications are inventoried," or "Develop and implement a process to ensure the timely receipt of threat intelligence from [name of specific information sharing forums and sources]."
Risk Owner	The designated party responsible and accountable for ensuring that the risk is maintained in accordance with enterprise requirements. The risk owner may work with a designated risk manager who is responsible for managing and monitoring the selected risk response.
Status	A field for tracking the current condition of the risk and any next activities.

Figure 11 Desription for the fields on the risk register example (Quinn et al., 2023. pp. 26-27).

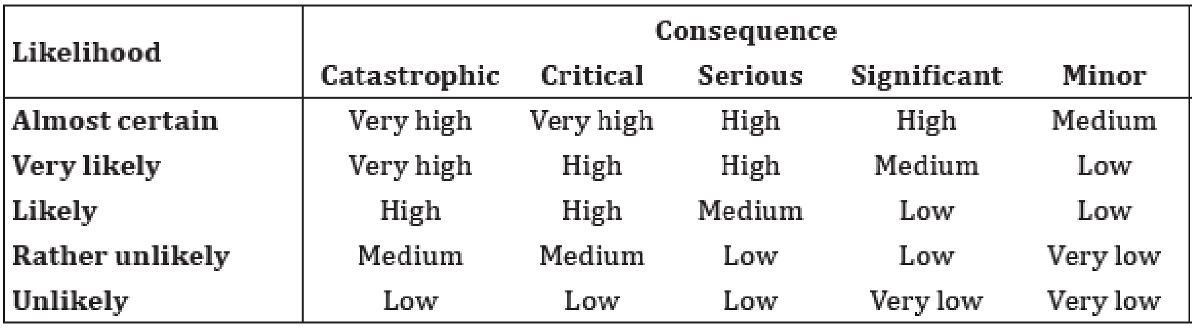
At least key threats must be identified for the organisations' critical assets or information. Data for the threats should be collected from the organisation's PESTLE analysis, a variety of threat databases, or threat reports, in example ASSA ABLOY's report on protecting your data against physical threats (ASSA ABLOY, 2024). Threats can be accidental, deliberate, or environmental. Based on the survey conducted by Finnish Digital and Population Data Services Agency's on autumn 2021 (DVV, 2021), one of the highest risk claims was seen as deliberate cyber security attacks on the public authorities' services as show in Figure 12. (DVV, 2021; Zhang & He, 2021).



Risk claim number	Risk claim	Risk score	Probability
2	Deliberate and serious security attacks on public authorities and services.	5,3	2,2
3	Critical physical infrastructure and cyber networks are subject to serious misuse, hacking, sabotage or security attacks.	5,2	2,0
25	Failure to manage the complexity of the IT department's cross-industry processes, ICT suppliers, subcontractors and production environments, resulting in disruption and service outages.	4,8	2,2
4	The security of information assets is significantly compromised, mainly due to urgency and lack of resources.	4,7	2,0
13	The excessiveness, lack of timeliness, inaccuracy, rapidity of change or other characteristics of the quality of the regulations, rules and guidance impose disproportionate obligations.	4,6	2,3
35	The risks of cloud services are not sufficiently understood, resulting in a lack of clarity on how to manage them - either through contracts or other means - and a lack of situational awareness.	4,6	2,1
23	Not enough financial resources have been allocated to digital security.	4,5	2,2
24	Not enough digital security expertise is available.	4,5	2,2
31	After a disruption, data cannot be made available again, meaning that data, intellectual property rights or software are lost.	4,3	1,7
29	Digital security is not understood, valued or taken into account in operational planning.	4,2	2,0

Figure 12 Top 10 risk claims, all responds (DVV, 2021).

The identified risks affecting vulnerabilities must be evaluated in the risk register, what is the level of the likelihood and impact of the risk. In qualitative risk assessment the risk criteria levels can be described with words and numeral ratings, and they can have colour descriptions. In example likelihood and impact (consequence) of the risk will have a described levels with words as shown in Figure 13. Levels in the qualitive risk assessment should be described as efficient as possible, so they will be uniform and everyone doing the risk assessment will understand the levels. In qualitative risk assessment method, the risk likelihood and impact levels can be based on the organisation's own needs. (ISO/IEC 27005, 2022; Patiño et al., 2018).



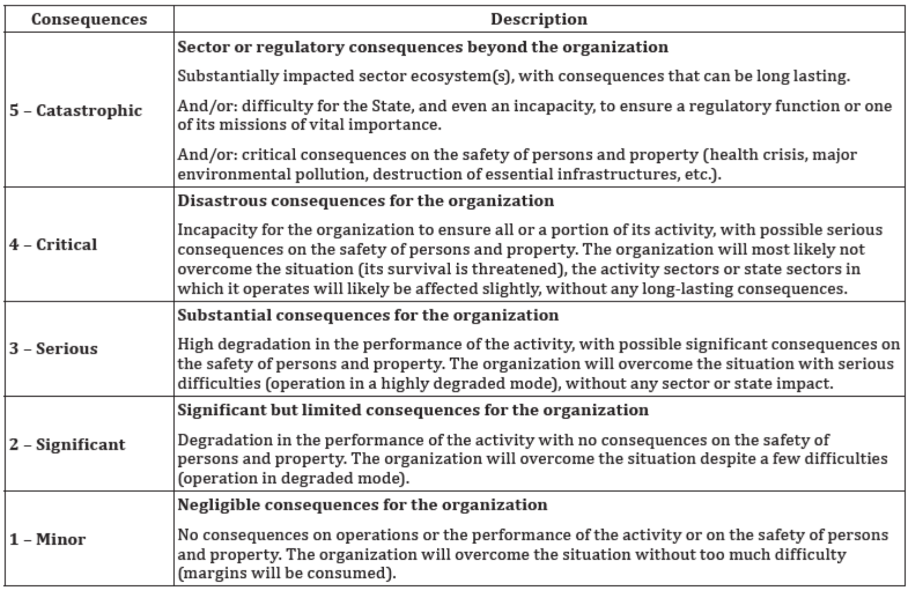
Likelihood	Consequence				
	Catastrophic	Critical	Serious	Significant	Minor
Almost certain	Very high	Very high	High	High	Medium
Very likely	Very high	High	High	Medium	Low
Likely	High	High	Medium	Low	Low
Rather unlikely	Medium	Medium	Low	Low	Very low
Unlikely	Low	Low	Low	Very low	Very low

Figure 13 Qualititative risk matrix levels described (ISO/IEC 27005, 2022, p. 113).

Organisation should describe risk criterion levels of the impact and likelihood of the risk, which can be employed on the risk register. Risk likelihood and impact levels can be based on the information confidentiality, integrity and operational availability of the information or the asset, or the value of the asset and on the related threats to the assets. (Kusprasapta & Putra, 2021; Alwi & Ariffin, 2018).

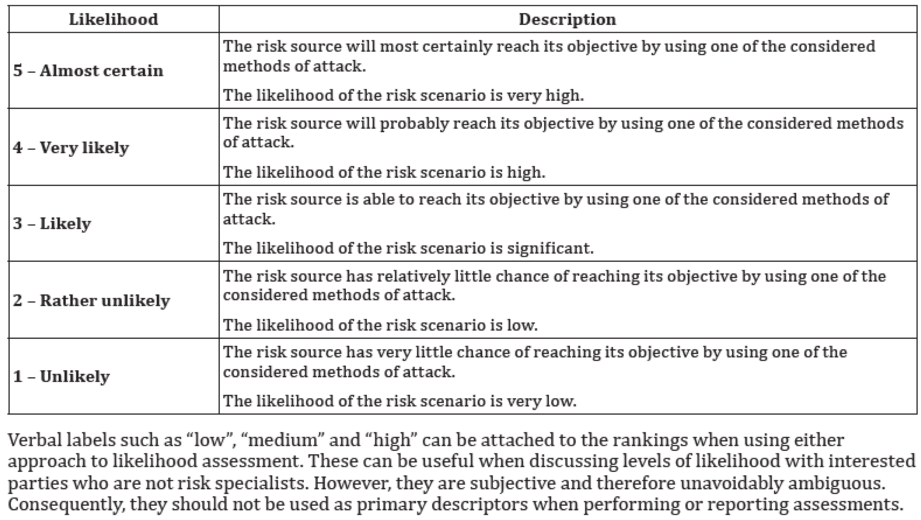
The risk impact criterion level should describe what kind level of damage the risk would have on the information or to the asset. Likelihood criterion level should describe how frequently the risk can happen. Risk likelihood and impact criterion level descriptions can described as shown in ISO27005 risk management examples Figures 14 and 15. Risk level should be graded and described based on the likelihood and impact level of the risk and based as shown in risk matrix example Figure 13. (Kusprasapta & Putra, 2021).

Identified and graded risks must have a risk treatment method, and based on that the organisation can choose proper security controls to mitigate the risk level or describe on how to maintain it and accept the risk level. Maintaining or changing controls to the risk is part of the risk management process. Organisation should have risk acceptance criterion for the risks, and it should describe when the risk is acceptable or not. The risk acceptance criterion level can be related to the organisation's goals or policies. In example very high and high risks must all the time be mitigated, medium risks can be mitigated, and low and very low risks can be accepted. Risk should have an owner who accepts the risk level or the chosen mitigations for the risk. (Anang et al., 2021; Kusprasapta & Putra, 2021).



Consequences	Description
5 – Catastrophic	**Sector or regulatory consequences beyond the organization** Substantially impacted sector ecosystem(s), with consequences that can be long lasting. And/or: difficulty for the State, and even an incapacity, to ensure a regulatory function or one of its missions of vital importance. And/or: critical consequences on the safety of persons and property (health crisis, major environmental pollution, destruction of essential infrastructures, etc.).
4 – Critical	**Disastrous consequences for the organization** Incapacity for the organization to ensure all or a portion of its activity, with possible serious consequences on the safety of persons and property. The organization will most likely not overcome the situation (its survival is threatened), the activity sectors or state sectors in which it operates will likely be affected slightly, without any long-lasting consequences.
3 – Serious	**Substantial consequences for the organization** High degradation in the performance of the activity, with possible significant consequences on the safety of persons and property. The organization will overcome the situation with serious difficulties (operation in a highly degraded mode), without any sector or state impact.
2 – Significant	**Significant but limited consequences for the organization** Degradation in the performance of the activity with no consequences on the safety of persons and property. The organization will overcome the situation despite a few difficulties (operation in degraded mode).
1 – Minor	**Negligible consequences for the organization** No consequences on operations or the performance of the activity or on the safety of persons and property. The organization will overcome the situation without too much difficulty (margins will be consumed).

Figure 14 Example of describing impact levels (ISO/IEC 27005, 2022, p. 111).



Likelihood	Description
5 – Almost certain	The risk source will most certainly reach its objective by using one of the considered methods of attack. The likelihood of the risk scenario is very high.
4 – Very likely	The risk source will probably reach its objective by using one of the considered methods of attack. The likelihood of the risk scenario is high.
3 – Likely	The risk source is able to reach its objective by using one of the considered methods of attack. The likelihood of the risk scenario is significant.
2 – Rather unlikely	The risk source has relatively little chance of reaching its objective by using one of the considered methods of attack. The likelihood of the risk scenario is low.
1 – Unlikely	The risk source has very little chance of reaching its objective by using one of the considered methods of attack. The likelihood of the risk scenario is very low.

Verbal labels such as “low”, “medium” and “high” can be attached to the rankings when using either approach to likelihood assessment. These can be useful when discussing levels of likelihood with interested parties who are not risk specialists. However, they are subjective and therefore unavoidably ambiguous. Consequently, they should not be used as primary descriptors when performing or reporting assessments.

Figure 15 Example of describing likelihood levels (ISO/IEC 27005, 2022, p. 112).

2.7 Risk Management Process

One of the risk management principles is to understand the risk, apply mitigations to reduce it, and understand the risk tolerance in the organisation. Another essential risk management principle is to govern ownership of the risks. Risk management processes frequently use the Plan-Do-

Check-Act cycle, such as Deming's cycle, which can be used as a systematic process for continual improvement. The purpose of risk assessment and management is not all the time to achieve an operative environment with zero risks, but to bring those risks to the level of the organisation's risk acceptance. (Savolainen, 2023; Tsochev & Stankov, 2020)

Those risks are called residual risks, and the organisation needs to have methods to control those risks with proper security policies and measures. Residual risks affecting the assets which are not in level of the organisations' risk acceptance, should be included in the organisation's business continuity plan and in example a business impact analysis should be conducted. Continuity is vital for all organisations, and thus, with a proper risk management, the organisation can create a safer operative environment. (Savolainen, 2023; Tsochev & Stankov, 2020; Al-Essa & Al-Sharidah, 2018)

Organisations encounter new and complex security issues, which are frequently met with a proper risk management. Organisations should have a process to measure information security controls and have a continual improvement process. Integrating risk management processes for the organisation's security practices is not typically straightforward. Risk management should typically have enough information to form correct decisions, so having a framework to manage risks and using threat databases and reports to assess the risks is essential. Another challenge the risk management will face is that not all users have the proper knowledge to understand the threats affecting the organisation. Therefore, an organisation's risk management should be based on a specific framework and have enough information about the threats. (Boodai et al., 2022; Tsochev & Stankov, 2020; Sun et al., 2020).

2.8 Continual Improvement Process

The ISO 27001 and ISO 27005 standards offer a risk management process for organisations to use. One method for continual improvement in risk management is to use the PDCA (Plan-Do-Check-Act) four-step cycle, which is based on Deming's cycle, as mentioned prior. The PDCA cycle is frequently employed to improve processes with a continual approach, and it can be employed with almost any management or operative process. Edward Deming popularized the PDCA cycle in the 1950s. With the PDCA cycle, the organisation can ask itself is the process working, or does it need adjustment in the next cycle, and how to improve it, or if it should be replanned entirely. PDCA creates a continual improvement cycle, which goes around and around, and the purpose is to improve the process with each cycle. (Stefanova-Stoyanova & Danov, 2022; Pietrzak & Paliszkiewicz, 2015)

The Plan-Do-Check-Act cycle can be implemented using the ISO 27001 standard, which requires continual improvement of information management systems, including risk management and assessment. It includes planning, operation, performance evaluation, and improvement phases, and those can be linked to the PDCA cycle, as shown in Figure 16 (ISO/IEC 27001, 2022, Chapter 10. Improvement; Velasco et al., 2018)

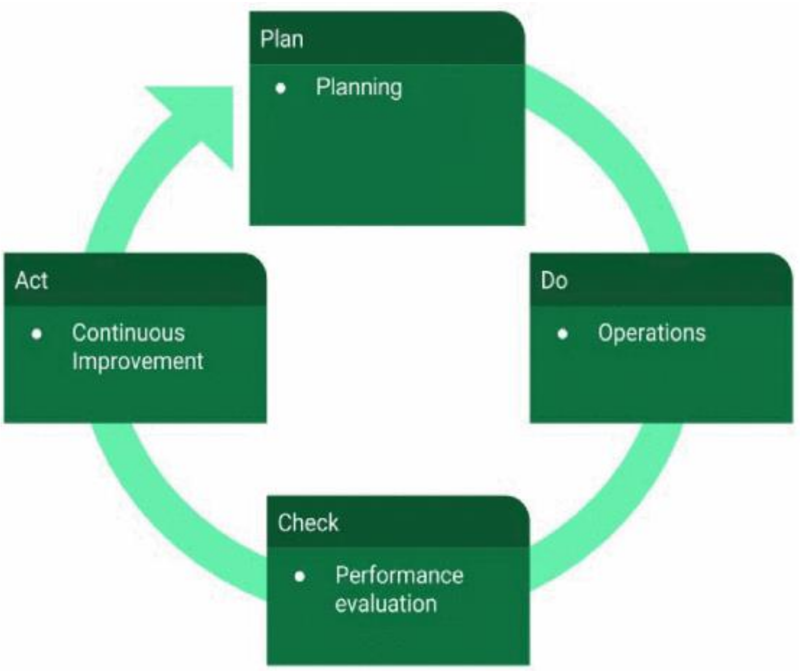


Figure 16 PDCA cycle ISO 27001:2013 (Velasco et al., 2018).

Throughout the planning phase (plan cycle), the organisation can plan and define the administrative area or secured area boundaries, specify what level of national classified information is handled and stored in the area, who is the owner of the area and select specific physical security controls based on the framework employed. (NSA, 2020, pp. 24-32; Carvalho & Marques, 2019; Velasco et al., 2018)

The planning phase in addition defines the risk assessment approach and what kind of risks affect the assets, processes, and information the organisation has evaluated as significant. Organisations can determine the risk level with likelihood and impact, as mentioned in the risk assessment section. The operation phase (do cycle) is to define the risk management, risk treatment plan and implement necessary controls and procedures to mitigate the risks. (Carvalho & Marques, 2019; Velasco et al., 2018)

The performance evaluation phase (Check cycle) evaluates and monitors the security controls and procedures employed to mitigate risks and monitor errors and security incidents. The evaluation phase should in addition include a review of the risks based on the changes in the threats, the organisation’s goals, and processes. The improvement phase (Act cycle) is to implement new security controls and procedures to mitigate the risk according to the evaluation results, or deploy business continual plan with business impact analysis, where performance evaluation did not give acceptable results. (ISO/IEC 27005, 2022, Chapter 10.8. Continual improvement; Carvalho & Marques, 2019; Velasco et al., 2018)

The PDCA cycles are part of the continual improvement process, and the organisation should have a plan on how frequently the continual improvement process is conducted and what are the criterion to start the cycle. The key criteria are materialisation of the risks and regulations or assets’ values are differentiating, in addition operative environment can change on how and where to store and handle national classified information, so these factors are a beneficial reason for the organisation to have a continual improvement with the PDCA cycle (ISO/IEC 27005, 2022, Chapter 10.8. Continual improvement; NSA, 2020, p. 11).

3 Implementation of the Tool

The first version of the deployment and management tool for security areas is built using Excel 2021, considering that users in the organisation can modify the tool's functions, security measure requirements, risk rating levels, risk criterion and PDCA cycle tasks as needed. An organisation can have own risk criterion and security requirements for defining security zones, so the tool was implemented with this in mind so that it could be modified for the organisation needs. An example of a tool use case is shown in Appendix 1.

3.1 Katakri 2020 Physical Requirements and Risk Management Processes

This tool version includes the brief Katakri 2020 physical security requirements for administrative and secured areas. Risk assessment and management processes are based on scientific articles and the ISO 270001 standard, which were retrieved for the theory background. Risk likelihood and impact levels are based on the ISO 27005 standard, and by default, there are three levels of risk rating scale: low, moderate, and high. The risk rating scale can be changed according to the organisation's needs.

Helsinki City uses the Finnish version of Office; therefore, the Excel formulas used in these Excel sheets are made with the Finnish version of Excel 2021. To get the Excel functions to work properly, the users must change the Excel interface language to Finnish or use an Excel functions translator. The Excel formulas used in the tool need Excel 2021 or a newer version.

3.2 Functions of the Tool

The default functions of the tool are separated into different numbered Excel worksheet tabs. The tool consists of seven function worksheets and one data worksheet, as shown in Figure 17, where most editable values are located, excluding the risk criterion descriptions placed on the risk criterion worksheet tab. Users can add functions to the tool according to organisation's needs, for example, a business impact analysis function for risks that could not be mitigated to the risk accepted level. By default, the data worksheet tab is hidden, in case that the organisation does not want that the end users alter the security measure requirements, list choices or risk rating levels.

The default worksheets are following:

- Data_Sheet
- Introduction
- Background
- Security measures
- Risk assessment
- Risk criterion
- Risk Management
- Continual improvement.

_Data_Sheet

1. Introduction

2. Background

3. Security measures

4. Risk assessment

5. Risk criterion

6. Risk management

7. Continual in ...

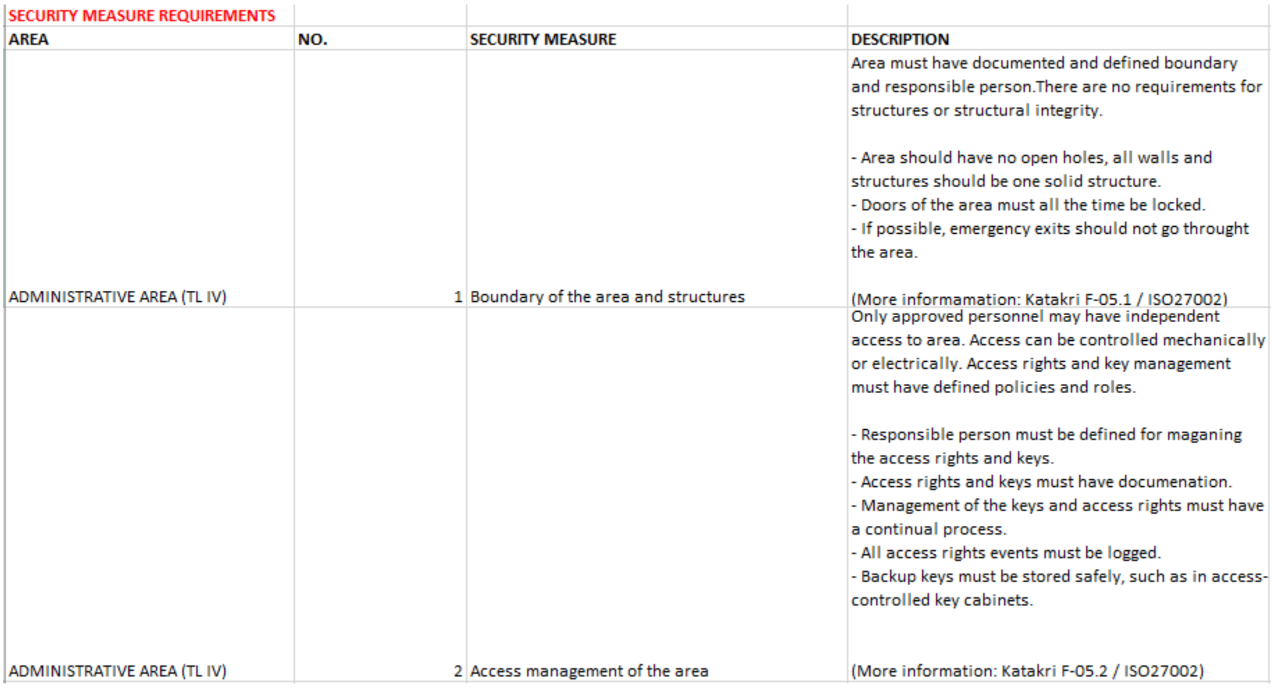
Figure 17 Worksheet tabs.

As the tool is implemented in Excel, some functions require users to perform manual actions, such as managing and mitigating new risks. The versioning of the security areas can be managed with different copies of Excel spreadsheets. It is advisable to create a new version of the Excel spreadsheet when the security measures in the area change, either being fulfilled with risk mitigation or new demands arise for the requirements. Because of this, the risks must be reassessed again. The automatic functions only work up to a certain point when filling out the risk assessment table.

3.2.1 Data tab

The data tab contains essentially all the editable data used in the tool's functions. Users in the organisation can edit the data as required; however, to keep the tool's usability consistent within the organisation, only named users should make changes to the values. The editable information includes the following items: security level, security measure selection, security policy requirements, risk impact, and probability levels, and several list options.

Default security measure values use Katakri 2020’s physical security requirements and ISO 27002 security requirements, as shown in Figure 18. The requirements are described at the general level, so users should have a general knowledge of the Katakri’s physical security requirements and ISO27002 standard when using the default requirements. However, the description of the security requirements also includes references to more specific requirements. The Helsinki City rescue services have their requirements for security measures, which will be used with the tool.



SECURITY MEASURE REQUIREMENTS

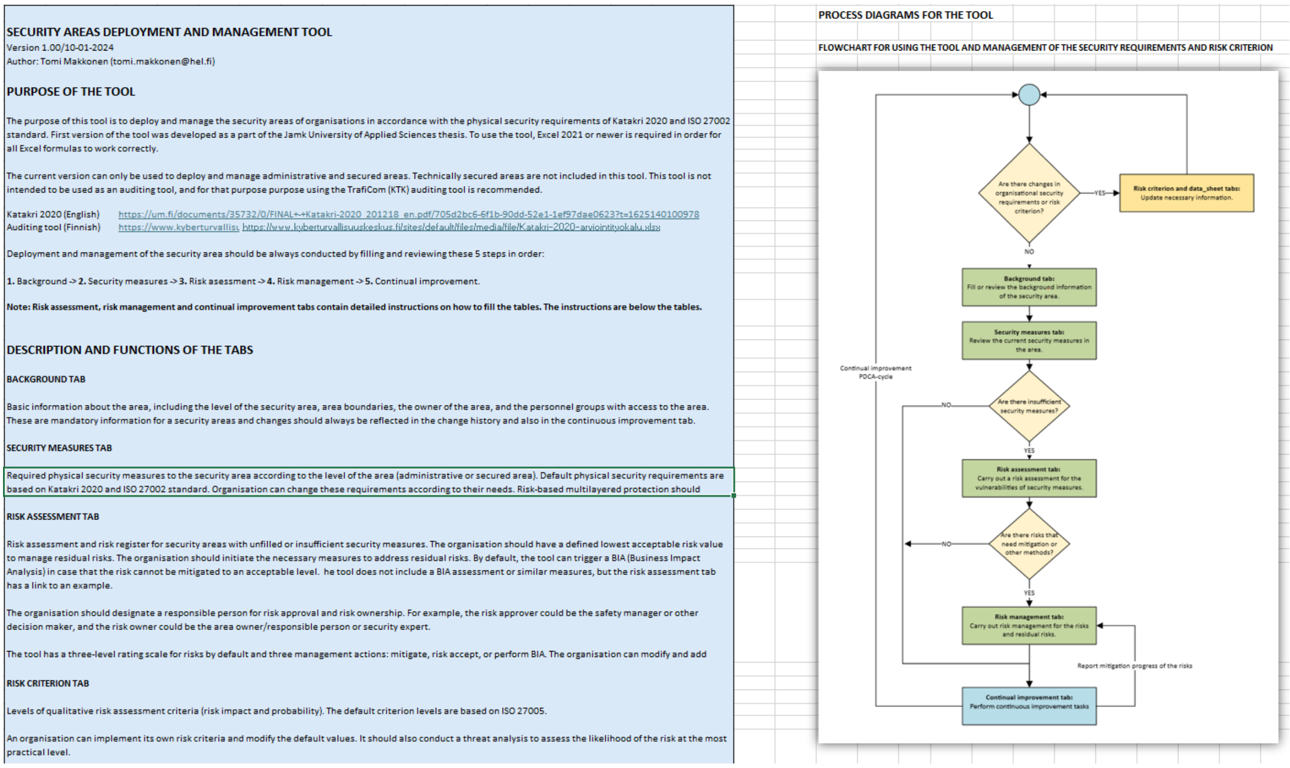
AREA	NO.	SECURITY MEASURE	DESCRIPTION
ADMINISTRATIVE AREA (TL IV)	1	Boundary of the area and structures	Area must have documented and defined boundary and responsible person.There are no requirements for structures or structural integrity. - Area should have no open holes, all walls and structures should be one solid structure. - Doors of the area must all the time be locked. - If possible, emergency exits should not go throught the area. (More informamation: Katakri F-05.1 / ISO27002)
ADMINISTRATIVE AREA (TL IV)	2	Access management of the area	Only approved personnel may have independent access to area. Access can be controlled mechanically or electrically. Access rights and key management must have defined policies and roles. - Responsible person must be defined for maganing the access rights and keys. - Access rights and keys must have documenation. - Management of the keys and access rights must have a continual process. - All access rights events must be logged. - Backup keys must be stored safely, such as in access-controlled key cabinets. (More information: Katakri F-05.2 / ISO27002)

Figure 18 Modifiable security measure requirements in the data sheet tab.

3.2.2 Introduction tab

The introductory tab includes the version, introductions, and process diagrams on using the tool, which explains the tool's purpose and functionalities, as shown in Figure 19. Guidelines may be adapted as necessary to meet the organisation's needs.

The user should start from the background information tab and continue to fill in the tool procedurally as shown in the tool’s flowchart, as shown in Figure 19. Deployment and management of the security areas should always be conducted by filling out and reviewing the worksheet tabs in a specific order, as explained in the introduction worksheet tab.



SECURITY AREAS DEPLOYMENT AND MANAGEMENT TOOL
Version 1.00/10-01-2024
Author: Tomi Makkonen (tomi.makkonen@hel.fi)

PURPOSE OF THE TOOL

The purpose of this tool is to deploy and manage the security areas of organisations in accordance with the physical security requirements of Katakri 2020 and ISO 27002 standard. First version of the tool was developed as a part of the Jamk University of Applied Sciences thesis. To use the tool, Excel 2021 or newer is required in order for all Excel formulas to work correctly.

The current version can only be used to deploy and manage administrative and secured areas. Technically secured areas are not included in this tool. This tool is not intended to be used as an auditing tool, and for that purpose purpose using the TrafiCom (KTK) auditing tool is recommended.

Katakri 2020 (English) https://um.fi/documents/35732/0/FINAL+-+Katakri-2020_201218_en.pdf/705d2bc6-6f1b-90dd-52e1-1ef97dae0623?t=1625140100978
Auditing tool (Finnish) https://www.kyberturvallisu https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Katakri-2020-arviointityokalu.xlsx

Deployment and management of the security area should be always conducted by filling and reviewing these 5 steps in order:

1. Background -> **2.** Security measures -> **3.** Risk asessment -> **4.** Risk management -> **5.** Continual improvement.

Note: Risk assessment, risk management and continual improvement tabs contain detailed instructions on how to fill the tables. The instructions are below the tables.

DESCRIPTION AND FUNCTIONS OF THE TABS

BACKGROUND TAB

Basic information about the area, including the level of the security area, area boundaries, the owner of the area, and the personnel groups with access to the area. These are mandatory information for a security areas and changes should always be reflected in the change history and also in the continuous improvement tab.

SECURITY MEASURES TAB

Required physical security measures to the security area according to the level of the area (administrative or secured area). Default physical security requirements are based on Katakri 2020 and ISO 27002 standard. Organisation can change these requirements according to their needs. Risk-based multilayered protection should

RISK ASSESSMENT TAB

Risk assessment and risk register for security areas with unfilled or insufficient security measures. The organisation should have a defined lowest acceptable risk value to manage residual risks. The organisation should initiate the necessary measures to address residual risks. By default, the tool can trigger a BIA (Business Impact Analysis) in case that the risk cannot be mitigated to an acceptable level. he tool does not include a BIA assessment or similar measures, but the risk assessment tab has a link to an example.

The organisation should designate a responsible person for risk approval and risk ownership. For example, the risk approver could be the safety manager or other decision maker, and the risk owner could be the area owner/responsible person or security expert.

The tool has a three-level rating scale for risks by default and three management actions: mitigate, risk accept, or perform BIA. The organisation can modify and add

RISK CRITERION TAB

Levels of qualitative risk assessment criteria (risk impact and probability). The default criterion levels are based on ISO 27005.

An organisation can implement its own risk criteria and modify the default values. It should also conduct a threat analysis to assess the likelihood of the risk at the most practical level.

PROCESS DIAGRAMS FOR THE TOOL

FLOWCHART FOR USING THE TOOL AND MANAGEMENT OF THE SECURITY REQUIREMENTS AND RISK CRITERION

Are there changes in organisational security requirements or risk criterion?
YES
Risk criterion and data_sheet tabs: Update necessary information.
NO
Background tab: Fill or review the background information of the security area.
Security measures tab: Review the current security measures in the area.
Continual improvement PDCA-cycle
Are there insufficient security measures?
NO
YES
Risk assessment tab: Carry out a risk assessment for the vulnerabilities of security measures.
Are there risks that need mitigation or other methods?
NO
YES
Risk management tab: Carry out risk management for the risks and residual risks.
Report mitigation progress of the risks
Continual improvement tab: Perform continuous improvement tasks

Figure 19 Introduction to the tool and flowchart to guide user.

3.2.3 Background tab

The background tab contains the administrative details of the security area, defining the boundaries of the security area and the owner of the area and selecting corresponding level of the security area. Other important information includes the persons or groups of persons who have access to the security perimeter and the history of changes to the perimeter. In principle, the site owner is responsible for the planning, management and continuous improvement of the security area, but should also be jointly managed on operational level.

Security area can be defined with this tool per floor of the building, per room or per individual room. It is up to the organisation to decide at which level it wants to describe the security areas with this tool. In principle, the tool works best when describing individual spaces or rooms boundaries, as shown in the Figure 20.

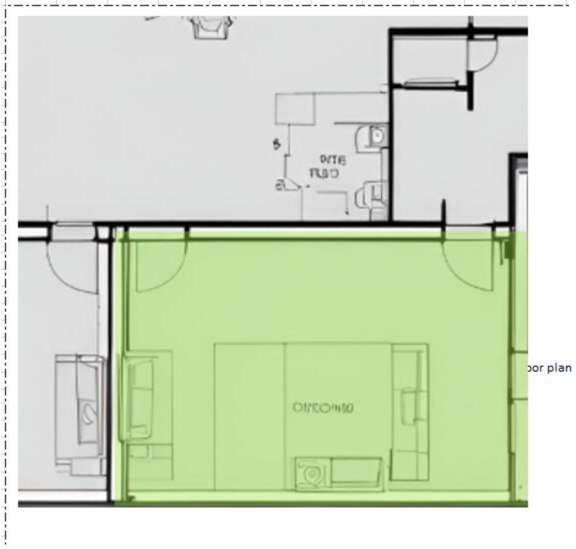
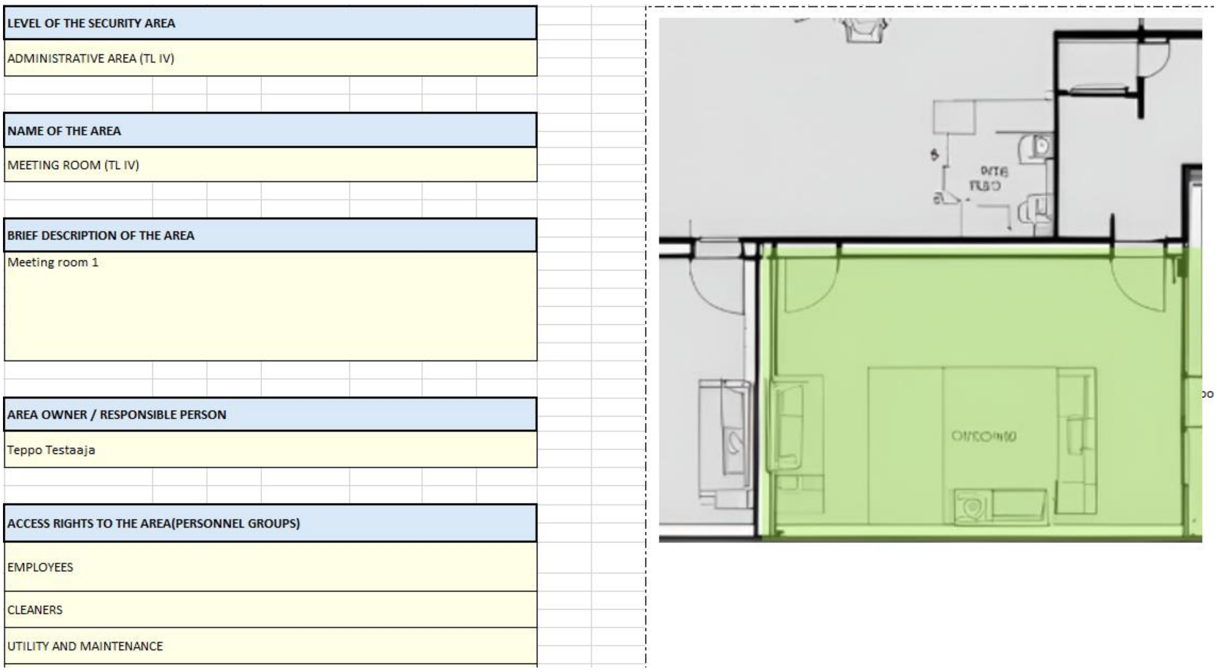


Figure 20 An example of floor plans which is defined as an administrative area.

When planning and deploying a security area, consideration should be given to the level of national classified information that will be handled and stored there, and whether the area has an important assets like server or active network devices for the organisation. In the example, organisation decides that the area is an administrative area, so the level of security area is selected as an administrative area, as shown in the Figure 21.

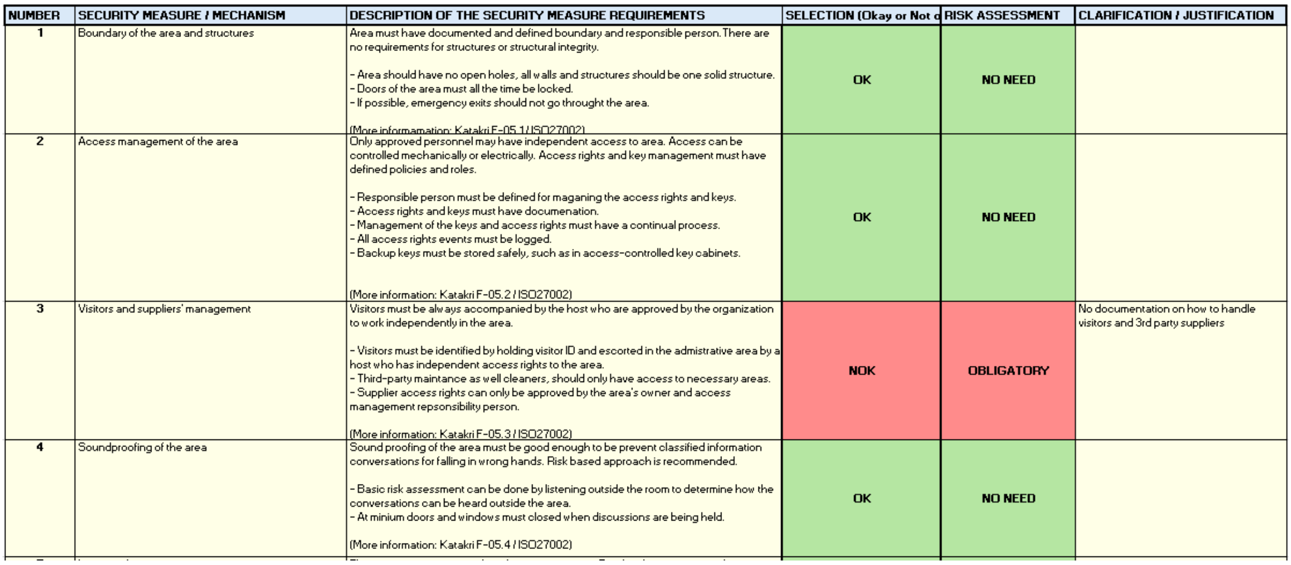


LEVEL OF THE SECURITY AREA
ADMINISTRATIVE AREA (TL IV)
NAME OF THE AREA
MEETING ROOM (TL IV)
BRIEF DESCRIPTION OF THE AREA
Meeting room 1
AREA OWNER / RESPONSIBLE PERSON
Teppo Testaaja
ACCESS RIGHTS TO THE AREA(PERSONNEL GROUPS)
EMPLOYEES
CLEANERS
UTILITY AND MAINTENANCE

Figure 21 An example of the background information of the area.

3.2.4 Security Measures tab

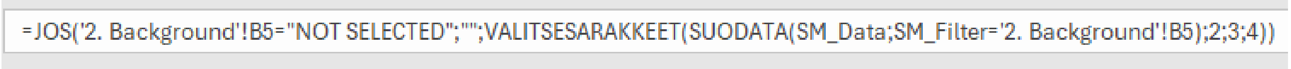
Based on the selection of the level of area the security measure requirements are fetch to this tab from the data sheet. The user selects at each security measure requirements whether the safety requirement is okay or not okay. In this version, all requirements are mandatory, so any insufficient safety requirements are taken to the risk assessment tab.



NUMBER	SECURITY MEASURE / MECHANISM	DESCRIPTION OF THE SECURITY MEASURE REQUIREMENTS	SELECTION (Okay or Not o	RISK ASSESSMENT	CLARIFICATION / JUSTIFICATION
1	Boundary of the area and structures	Area must have documented and defined boundary and responsible person. There are no requirements for structures or structural integrity. - Area should have no open holes, all walls and structures should be one solid structure. - Doors of the area must all the time be locked. - If possible, emergency exits should not go throught the area. (More informamation: Katakri F-05.1 / ISO27002)	OK	NO NEED	
2	Access management of the area	Only approved personnel may have independent access to area. Access can be controlled mechanically or electrically. Access rights and key management must have defined policies and roles. - Responsible person must be defined for maganing the access rights and keys. - Access rights and keys must have documenation. - Management of the keys and access rights must have a continual process. - All access rights events must be logged. - Backup keys must be stored safely, such as in access-controlled key cabinets. (More information: Katakri F-05.2 / ISO27002)	OK	NO NEED	
3	Visitors and suppliers' management	Visitors must be always accompanied by the host who are approved by the organization to work independently in the area. - Visitors must be identified by holding visitor ID and escorted in the admistrative area by a host who has independent access rights to the area. - Third-party maintance as well cleaners, should only have access to necessary areas. - Supplier access rights can only be approved by the area's owner and access management repsonsibility person. (More information: Katakri F-05.3 / ISO27002)	NOK	OBLIGATORY	No documentation on how to handle visitors and 3rd party suppliers
4	Soundproofing of the area	Sound proofing of the area must be good enough to be prevent classified information conversations for falling in wrong hands. Risk based approach is recommended. - Basic risk assessment can be done by listening outside the room to determine how the conversations can be heard outside the area. - At minium doors and windows must closed when discussions are being held. (More information: Katakri F-05.4 / ISO27002)	OK	NO NEED	

Figure 22 Filling out security measure requirements for the administrative area.

Specific Excel-formula is in place to retrieve the security measure requirements from the data sheet. The formula is using IF, CHOOSECOLS and FILTER functions, however in this version the functions are in Finnish, as show in Figure 23.

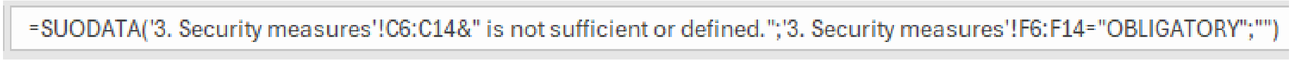


```
=JOS('2. Background'!B5="NOT SELECTED";"";VALITSESARAKKEET(SUODATA(SM_Data;SM_Filter='2. Background'!B5);2;3;4))
```

Figure 23 Excel-formula to fetch security measure requirements based on the selection.

3.2.5 Risk Assessment tab

Risk assessment vulnerabilities columns are filled automatically when the security measure requirements are not sufficient. The Excel-formula used to fetch the insufficient security measure requirements is using FILTER-function, as shown in Figure 24.

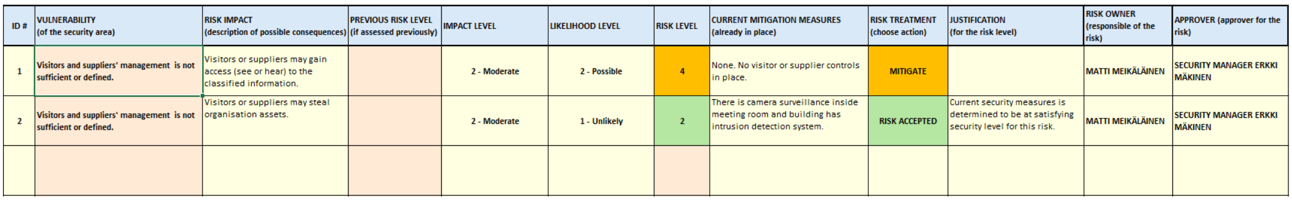


```
=SUODATA('3. Security measures'!C6:C14&" is not sufficient or defined.";'3. Security measures'!F6:F14="OBLIGATORY";"")
```

Figure 24 Excel-formula to fetch unsufficient security measures.

Based on the theory background, the organisation must evaluate risks which may affect the vulnerability. Organisation should identify key risks affecting the vulnerabilities from their own threat analysis or by using different threat databases or reports. Vulnerabilities may have several risks, so the user must manually copy & paste a new row. Ther risk assessment table is based on this thesis's theory background and the columns are following, as shown in the Figure 25.

- ID (ID of the risk)
- Vulnerability (Security measure which is insufficient or not okay)
- Risk impact (Description of the possible consequences)
- Previous risk level (Risk level whether assessed previously)
- Impact level (Impact level of the risk)
- Likelihood level (Likelihood level of the risk)
- Risk level (Risk level is impact times likelihood)
- Current mitigation measures (Current mitigation measures in place to justify risk level or need for mitigation)
- Risk treatment (Accept, mitigate or conduct a business impact analysis)
- Justification (Justification for the risk level)
- Risk owner (Risk owner is the person who takes ownership of the risk and continues with mitigation).
- Approver (Approver is the person who approves the risk)

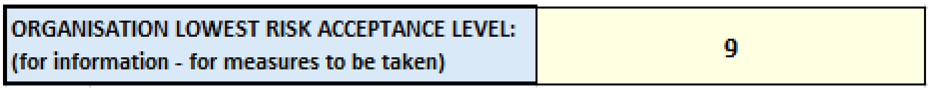


ID #	VULNERABILITY (of the security area)	RISK IMPACT (description of possible consequences)	PREVIOUS RISK LEVEL (if assessed previously)	IMPACT LEVEL	LIKELIHOOD LEVEL	RISK LEVEL	CURRENT MITIGATION MEASURES (already in place)	RISK TREATMENT (choose action)	JUSTIFICATION (for the risk level)	RISK OWNER (responsible of the risk)	APPROVER (approver for the risk)
1	Visitors and suppliers' management is not sufficient or defined.	Visitors or suppliers may gain access (see or hear) to the classified information.		2 - Moderate	2 - Possible	4	None. No visitor or supplier controls in place.	MITIGATE		MATTI MEIKÄLÄINEN	SECURITY MANAGER ERKKI MÄKINEN
2	Visitors and suppliers' management is not sufficient or defined.	Visitors or suppliers may steal organisation assets.		2 - Moderate	1 - Unlikely	2	There is camera surveillance inside meeting room and building has intrusion detection system.	RISK ACCEPTED	Current security measures is determined to be at satisfying security level for this risk.	MATTI MEIKÄLÄINEN	SECURITY MANAGER ERKKI MÄKINEN

Figure 25 Example risks for the vulnerabilities.

Risk assessment tab also provides further guidance to users. There are no automation features for adding new risks affecting vulnerabilities, therefore user must copy & paste selected vulnerabilities as a new row under the already defined rows. By default, the risk treatment selection offers three actions for the risks which are acceptance of the risk, mitigation or conducting a business impact analysis for risks which cannot be mitigated to accepted level.

The tab also contains a risk acceptance level definition for organisations, as show in Figure 26. A figure can be placed to indicate when a risk requires separate action, such as a business impact analysis. Risk acceptance level definition has no functions, but it’s meant to be used an indication when to act on risks with planned actions.

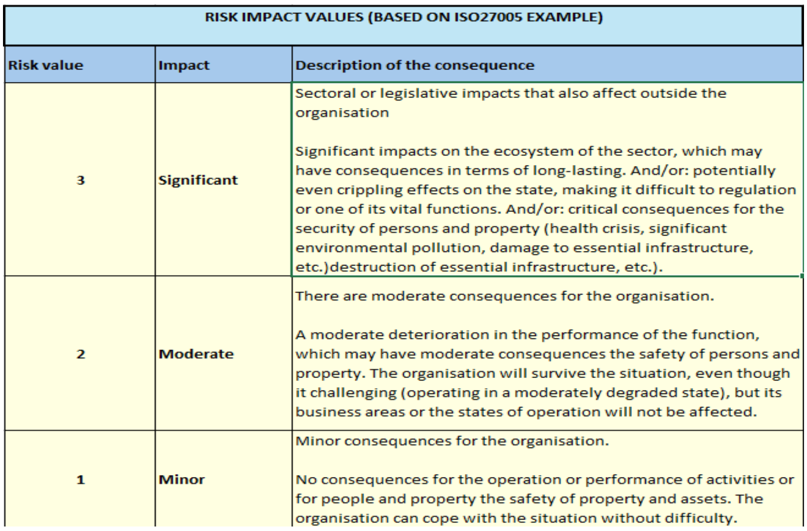


ORGANISATION LOWEST RISK ACCEPTANCE LEVEL: (for information - for measures to be taken)	9

Figure 26 Example of organisation risk acceptance level.

3.2.6 Risk Criteron tab

The tool has a separate risk criteria tab where users can describe the impact and likelihood of a risk and the risk level scale. The tool includes a simplified three-level evaluation for risks using a risk criterion based on the ISO27001 standard. The qualitative values are explained with qualitative numbers and text, as shown in Figure 27. The organisation can change the descriptions of the risk criteria to meet their needs. The changes should also be reflected in the data sheet tab. Thus, the values are available for risk assessment.

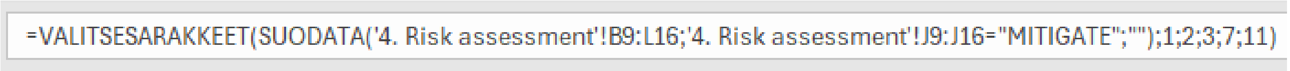


RISK IMPACT VALUES (BASED ON ISO27005 EXAMPLE)		
Risk value	Impact	Description of the consequence
3	Significant	Sectoral or legislative impacts that also affect outside the organisation Significant impacts on the ecosystem of the sector, which may have consequences in terms of long-lasting. And/or: potentially even crippling effects on the state, making it difficult to regulation or one of its vital functions. And/or: critical consequences for the security of persons and property (health crisis, significant environmental pollution, damage to essential infrastructure, etc.)destruction of essential infrastructure, etc.).
2	Moderate	There are moderate consequences for the organisation. A moderate deterioration in the performance of the function, which may have moderate consequences the safety of persons and property. The organisation will survive the situation, even though it challenging (operating in a moderately degraded state), but its business areas or the states of operation will not be affected.
1	Minor	Minor consequences for the organisation. No consequences for the operation or performance of activities or for people and property the safety of property and assets. The organisation can cope with the situation without difficulty.

Figure 27 Risk impact values.

3.2.7 Risk Management tab

The risk management tab handles all risks that need mitigation, as selected in the risk assessment tab. Risks are automatically retrieved for the mitigation table from the risk assessment with the Excel formula, which has the following columns: ID, vulnerability, risk impact, risk level, and risk owner, as shown in Figure 28. The Excel formula uses a combination of CHOOSECOLS and FILTER functions.



```
=VALITSESARAKKEET(SUODATA('4. Risk assessment'!B9:L16;'4. Risk assessment'!J9:J16="MITIGATE";"");1;2;3;7;11)
```

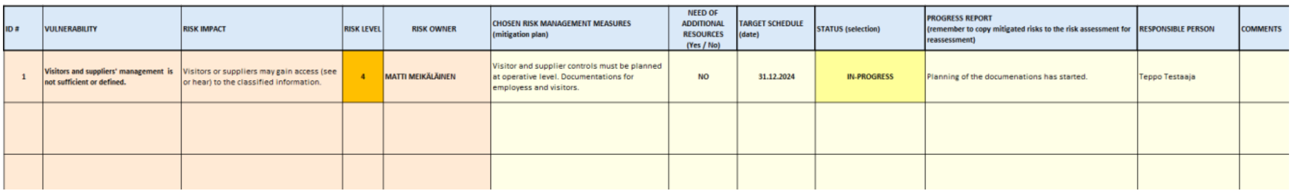
Figure 28 Excel-formula to fetch risks which need mitigation.

Mitigation table for risks includes automatically fetched values as stated above, but the rest of the columns must be filled manually which includes following:

- chosen risk management measures (mitigation plans)
- need of additional resources (yes or no)
- target Schedule (date)
- status on implementation (selection: not yet started, in-progress, completed)
- progress report
- responsible person (by default responsible person is the area owner)
- comments.

The risk owner with the responsible person should describe in as much detail as possible the feasible risk management methods that will be used to mitigate the risk. The owner should also decide whether additional resources are needed for the measures and write a note in the comments. A target timetable for the implementation of the risk management measures must be defined and the progress must be monitored and reported. An example of filled mitigation table is shown in Figure 29.

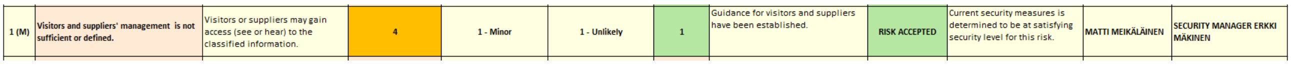
Monitoring and reporting of the implementation of the risk management measures is explained in more details in the section “3.2.8 Continual improvement worksheet tab” as it is part of the continual improvement cycle.



ID #	VULNERABILITY	RISK IMPACT	RISK LEVEL	RISK OWNER	CHOSEN RISK MANAGEMENT MEASURES (mitigation plan)	NEED OF ADDITIONAL RESOURCES (Yes / No)	TARGET SCHEDULE (date)	STATUS (selection)	PROGRESS REPORT (remember to copy mitigated risks to the risk assessment for reassessment)	RESPONSIBLE PERSON	COMMENTS
1	**Visitors and suppliers' management is not sufficient or defined.**	Visitors or suppliers may gain access (see or hear) to the classified information.	4	MATTI MEIKÄLÄINEN	Visitor and supplier controls must be planned at operative level. Documentations for employess and visitors.	NO	31.12.2024	IN-PROGRESS	Planning of the documenations has started.	Teppo Testaaja	

Figure 29 An example of the mitigation table.

Mitigated risks must be manually copied to the risk assessment tab as a new row below the assessed risks. The owner must assess the risk again, including the previous risk level in the row, as shown in Figure 30. In this use case, the same ID is used for the mitigated risk as for the original ID of the vulnerability, with an added (M) behind the ID to clarify the management of the risks. It is up to the organisation to decide on the labelling policy and how to identify mitigated risks that are consistent with the original risk.



1 (M)	**Visitors and suppliers' management is not sufficient or defined.**	Visitors or suppliers may gain access (see or hear) to the classified information.	4	1 - Minor	1 - Unlikely	1	Guidance for visitors and suppliers have been established.	RISK ACCEPTED	Current security measures is determined to be at satisfying security level for this risk.	MATTI MEIKÄLÄINEN	SECURITY MANAGER ERKKI MÄKINEN

Figure 30 An example of mitigated risk brought to risk assessment tab.

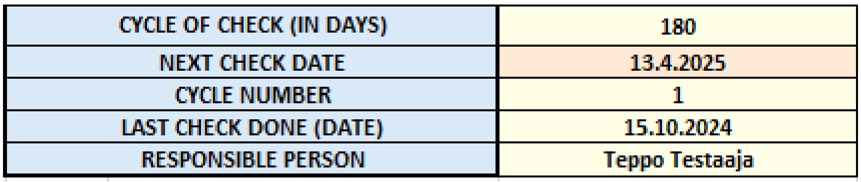
The risk owner and owner of the area should create a new version of the Excel spreadsheet whenever the risk management measures meet the security measures requirements for the security area and reassess the security measures again within the new version of the spreadsheet. From a version control point of view, this procedure is the best option for this Excel tool so that automatic functions do not break. In practice, this means that the user copies all the background information of the security area to the new empty version of the tool and reassesses the security requirements for the security area.

3.2.8 Continual Improvement tab

The process of continual improvement of the security area requires the most work from the area's owner. The continual improvement tab includes a simplified PDCA cycle to manage this process.

The tool provides a default list of tasks for the owner to go through the PDCA cycle, and with these tasks, the user can plan, do, check, and act on the changes.

By default, the parameters of the PDCA cycle are that the area owner is responsible for conducting the PDCA cycle of the security area, as shown in Figure 31. Six months (180 days) is the default span for carrying out the cycle, and the owner must increase the cycle number when the cycle is done. Organisations should decide their own cycle of checks for carrying out the PDCA cycle according to their demands.



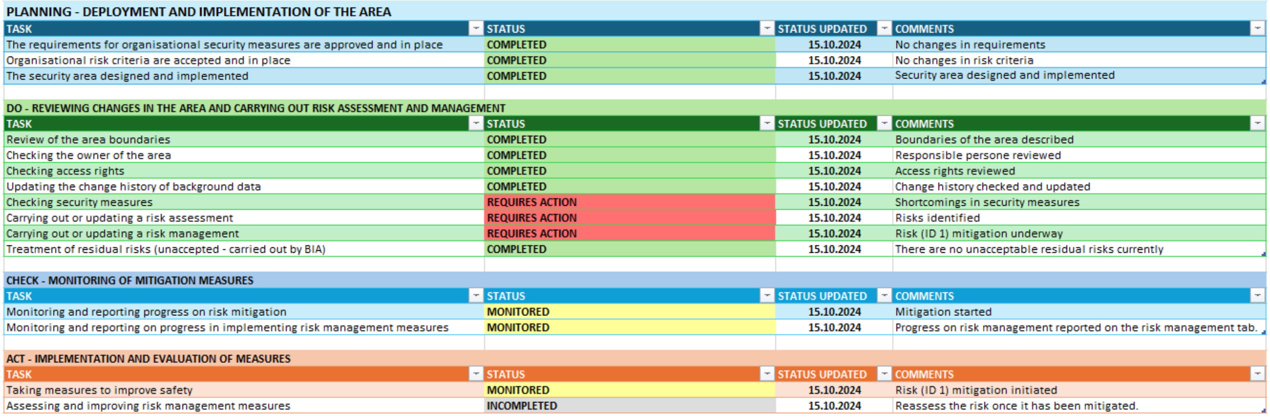
CYCLE OF CHECK (IN DAYS)	180
NEXT CHECK DATE	13.4.2025
CYCLE NUMBER	1
LAST CHECK DONE (DATE)	15.10.2024
RESPONSIBLE PERSON	Teppo Testaaja

Figure 31 An example of PDCA cycle parameters

The PDCA task list, by default, contains simplified tasks for the area owner to go through. The first time a security zone is planned and deployed, there will be more to complete in the task list because all the tasks must be updated. The task is described at the header level, and for each task, the status is selected from the list menu, the date is updated, and any necessary change comments are added to the task. The list menu of the status includes choices which are:

- Completed
- Completed – Changes
- Requires action
- Monitored
- Incompleted.

The principle behind the status is to inform in case there have been any changes or problems filling the task, and it can be commented on, as shown in Figure 32. In the example figure, the planning, do, check, and act has been done in one run. The change date must always be updated to the tasks when the area owner is going through the tasks.



PLANNING - DEPLOYMENT AND IMPLEMENTATION OF THE AREA

TASK	STATUS	STATUS UPDATED	COMMENTS
The requirements for organisational security measures are approved and in place	COMPLETED	15.10.2024	No changes in requirements
Organisational risk criteria are accepted and in place	COMPLETED	15.10.2024	No changes in risk criteria
The security area designed and implemented	COMPLETED	15.10.2024	Security area designed and implemented

DO - REVIEWING CHANGES IN THE AREA AND CARRYING OUT RISK ASSESSMENT AND MANAGEMENT

TASK	STATUS	STATUS UPDATED	COMMENTS
Review of the area boundaries	COMPLETED	15.10.2024	Boundaries of the area described
Checking the owner of the area	COMPLETED	15.10.2024	Responsible persone reviewed
Checking access rights	COMPLETED	15.10.2024	Access rights reviewed
Updating the change history of background data	COMPLETED	15.10.2024	Change history checked and updated
Checking security measures	REQUIRES ACTION	15.10.2024	Shortcomings in security measures
Carrying out or updating a risk assessment	REQUIRES ACTION	15.10.2024	Risks identified
Carrying out or updating a risk management	REQUIRES ACTION	15.10.2024	Risk (ID 1) mitigation underway
Treatment of residual risks (unaccepted - carried out by BIA)	COMPLETED	15.10.2024	There are no unacceptable residual risks currently

CHECK - MONITORING OF MITIGATION MEASURES

TASK	STATUS	STATUS UPDATED	COMMENTS
Monitoring and reporting progress on risk mitigation	MONITORED	15.10.2024	Mitigation started
Monitoring and reporting on progress in implementing risk management measures	MONITORED	15.10.2024	Progress on risk management reported on the risk management tab.

ACT - IMPLEMENTATION AND EVALUATION OF MEASURES

TASK	STATUS	STATUS UPDATED	COMMENTS
Taking measures to improve safety	MONITORED	15.10.2024	Risk (ID 1) mitigation initiated
Assessing and improving risk management measures	INCOMPLETED	15.10.2024	Reassess the risk once it has been mitigated.

Figure 32 An example of completed PDCA task list for new security area

The correct order to go through the PDCA tasks is to start from the planning phase and finish on the act phase, as shown in Figure 33. Planning tasks are always completed the first time when planning and deploying the security area and going through all the steps in the tool. For example, next time, there should be only changes to them when there is a significant change to the security area, or there are changes or new requirements for the security requirements, or the organisation changes the risk criterion. Also, it should be considered that new risks must be assessed and have a mitigation plan as appropriate.

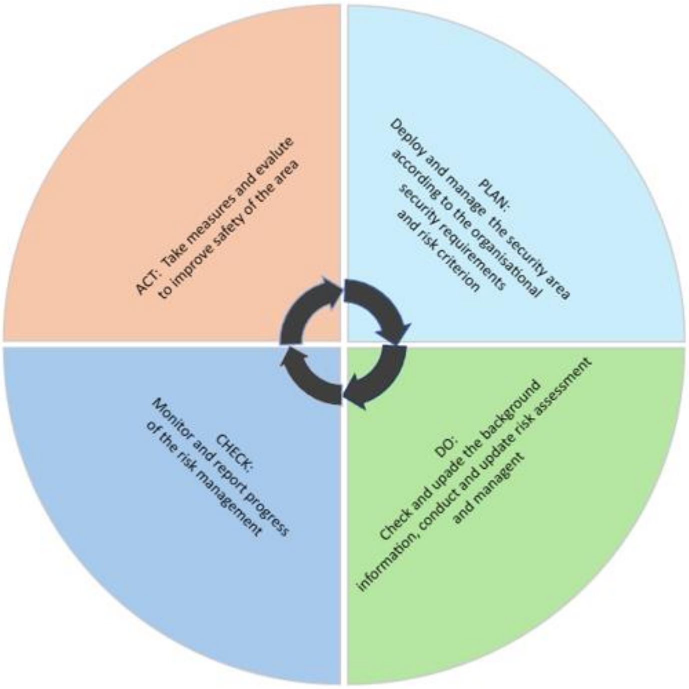

ACT: Take measures and evalute to improve safety of the area
PLAN: Deploy and manage the security area according to the organisational security requirements and risk criterion
CHECK: Monitor and report progress of the risk management
DO: Check and upade the background information, conduct and update risk assessment and managent

Figure 33 PDCA cycle

Do, Check, and Act tasks should be executed regularly before the deadline to ensure that changes to the security area are frequently reviewed and that the implementation of the mitigation for the risks is monitored and reported. Implemented mitigation measures should be evaluated, and action taken whenever they are not sufficient for the risk.

The PDCA cycle should not only be carried out before reaching the deadline. The continual improvement tab provides examples of when to start the PDCA cycle. For example, in realisation of the risk, the area owner should conduct the PDCA cycle and go through the task list. This is part of the act phase of the PDCA cycle.

4 Peer Interviews and Review of the Tool

Peer interviews were conducted with public and government security managers and security experts. Five interviews were conducted, and the interviews lasted an average of 45 minutes. The thesis researcher provided the interviewees with the latest version of the tool for testing and evaluation before the interviews. The interview included 15 questions on risk assessment, risk management, and continuous improvement, and the questions can be found in Appendix 1. The researcher recorded all interviews anonymously and analysed the responses afterward, resulting in a summary of the research questions, conclusions and ideas for further development.

5 Conclusions

Based on this research and development, a tool was developed to deploy and manage security areas according to the Katakri 2020 and ISO 27002 physical security requirements. The starting point has been to implement such a tool for Helsinki City rescue services, but also for national rescue services. The tool allows the owner of the area or security expert of the organisation to assess how safety requirements are being met. It also includes risk management and continuous improvement processes based on the collected theory background, to help maintain and improve the security of the area. The processes of the tool have been evaluated through peer interviews, which have allowed the tool's functionality to be assessed and research questions to be answered.

5.1 First Research Question

The first research question, ***"What is a suitable risk assessment and management method, and how should it be implemented in the tool?"*** was to find out what kind of risk assessment and risk management would work for the tool. Experts believe the tool's qualitative risk analysis is a good starting point for risk assessment, although it is always subjective. This means that the risk may not be assessed very accurately by just one expert or safety manager, but multiple perspectives are required when assessing risk qualitatively. The three-level rating scale used in the tool was considered sufficient for assessing physical security risks. Of course, there is always room for debate about the added value of a broader rating scale, but it depends mainly on what is being assessed. For example, in the case of information security risks, a five-level rating scale may be better in case the risk needs to be assessed at a more detailed level. The risk rating scale and risk criteria must, of course, be consistent with the organisation's needs, and organisations can customise these in the tool, which was found to be a good thing.

The experts felt that risk assessment should be as simple as possible, as it has often been found that a risk assessment that is too complex is not carried out. The risk assessment of the tool has taken into account all relevant information for the assessment and was seen as good and simple but still sufficiently comprehensive. The risk assessment needs to identify the risk, describe the consequences, and assess the impact and likelihood. It was also seen as a good thing that the tool automatically brings vulnerabilities in requirements to a risk assessment when a security requirement is not met.

The risk management measures were considered adequate and can be changed to the needs of the organisation. Highlighting BIA in the tool is a good thing for risks that are unacceptable to the organisation. ISO27001 and the NIS2 Directive require such measures from the organisations concerned. BIA is a useful tool in case risk cannot be sufficiently eliminated or mitigated. However, since risks are assessed subjectively, in some cases, BIA may be a too heavy measure for simple risks, and the organisation may have other methods for them.

The tool's risk management was seen to be sufficient, and there was good continuity with the risk assessment, as risks requiring action are automatically brought to the risk management. However, the experts made suggestions for improvement, and a response person for risk management measures should be indicated in the risk management tab. In the tool, this is by default the owner of the area, but the risk management table could have a separate field for this so that another responsible person could also be appointed. The suggestions for improvement have been taken into account in the latest version of the tool.

5.2 Second Research Question

In peer interviews with experts, continuous improvement and the PDCA cycle generated the most discussion. The second research question, ***"How should a continuous management process be implemented within the tool?"*** was to find out what kind of continuous improvement process would be good enough to be used with the tool. Experts found that the annual PDCA cycle is important for continuous improvement and well-suited for experts. It is an ISO27001 standard measure for continuous improvement. However, organisations may have their own methods for continuous improvement, so the use of the PDCA cycle in the tool may be less appropriate.

The experts saw the tool's continual improvement tasks as a good checklist for the owner of the area to check if there have been changes in the area or how risk management measures are progressing. The tasks are sensibly broken down; for example, the person in charge of the area or access rights may have changed, and the problem is only in one of them so that the change can be highlighted there. Initially, the PDCA cycle contained more tasks, but based on peer interviews, the tasks have been simplified and only leave the most essential tasks to go through. Colour coding was also added to the tasks' status selection to reflect better if a task triggers action.

5.3 Third Research Question

The third research question asked how useful this tool could be, ***"Is such a cross-functional tool, including risk management activities, useful for organisations that needs to consider physical security requirements and risks?"***. Based on the interviews, the researcher found that such a cross-functional tool is certainly helpful for organisations, as it is good to have a single tool to classify the security areas and assess security requirements and associated vulnerabilities. However, it should be noted that some organisations already have their own processes and tools for assessing and managing risks; in this case, the tool may not be suitable for such use. Such a tool will be handy for organisations that do not yet have procedures in place or wish to improve them. For a securityconscious organisation, a tool implemented with such precision is good and useful. The tool was found to be technical and may require training, as some manual operations require the user to have Excel skills. This, of course, depends on how well the user knows how to use Excel. Interviewees also raised the point that risk assessment tools are often expensive and not as comprehensive as this tool, so such a tool developed by the organisation itself is also useful in this respect.

6 Discussions

6.1 Possibilities for Further Research and Development

In terms of further research and development, it would certainly be useful to examine how NATO will affect the physical security of public authorities in the future, and it would also be useful to consider what aspects of the physical security of premises should be taken into account in emergency conditions. These aspects could be incorporated into this tool through further development, and the tool could also be used to include other areas that are not administrative or secured areas. The public administration evaluation criteria Julkri (Valtiovarainministeriö, 2023) can be used to introduce such other areas.

As for the tool's functionality, a dashboard view could be developed, where area owners can see how risk management measures are progressing. This would be beneficial when there are more risks, and the dashboard view would show the risks at a glance. In the future, the tool could also be integrated with other tools in the organisation if they exist for risk management. In addition, if the organisation had risk criteria in a central database, the tool could retrieve them from there.

6.2 Ethical Values and Reliability

The researcher followed JAMK's ethical values and principles (JAMK University of Applied Sciences, 2024). The fundamental ethical principles of the research are accountability, integrity, honesty, and respect. The researcher gathered all the information for the theory background from known databases or governmental and public administration publications. An artificial intelligence tool was used as an assistive tool in creating the example floor plans for the populated example of the tool.

The academic articles and publications used in the thesis are based on known knowledge of risk assessment and risk management based on ISO 27001 and NIST standards. The default values and processes used in the tool are based on academic publications and the physical security requirements of Katakri 2020, ISO 27001/27002, and NIST.

The researcher tested the usability of the tool with default values by deploying and managing a fictitious security area, which is also used as a populated example of the tool, as shown in Appendix 1. The usability of the tool was also reviewed with security experts, and views on the tool's functionality were collected through peer interviews. The tool was also presented to the TUVE project group of the Helsinki City rescue services and used to define the security areas of the organisation.

6.3 Researcher’s Reflections on the Thesis

The theoretical background is based on well-known safety frameworks and related scientific articles, so it was relatively straightforward to start establishing risk management functions in the tool using the background material collected from them. During the literature review, the most valuable insight was a better understanding of the significant differences between qualitative and quantitative risk assessment. It was also discovered that multiple experts should evaluate qualitative risk assessment because it is subjective.

As for the research methods, the peer interviews worked well and gave the researcher valuable feedback on the tool and answers to the research questions. In hindsight, the researcher could have interviewed the non-specialists and gained different insights on risk management. Such feedback can also be valuable as it can provide new insights. The researcher only received feedback from safety experts, whose responses were relatively consistent with the theoretical data collected. Nevertheless, the researcher was satisfied with the interview results and the target group selected. The results of the interviews provided good answers to the research questions and also suggestions for improvements to the tool itself.

The most important goal of this research and development was to develop a tool for the employer to manage security areas, which succeeded well. The structure of the thesis was intended to be coherent, beginning with an introduction of the employer, the research, and its problems, followed by a collection of theoretical background material for the tool and a description of the tool's functionalities. Finally, conclusions are presented, and opportunities for further research are highlighted.

In the researcher’s view, the thesis was successful. The most challenging part was writing the thesis in English, and sometimes, it wasn’t easy to find time to write because of life. In addition, implementing the tool in Excel created limitations for risk management functions. Not everything can be automated without using VBA, so the tool requires the user to have Excel skills. All in all, it can be said that writing the thesis was an educational journey and deepened the researcher’s knowledge of risk management.

6.4 How to Get Access to the Tool

The thesis researcher can be contacted directly by email tomi.makkonen@hel.fi in case that you have any questions about the tool or how to get access to it. For rescue services or other national authorities using the government security network, more specific physical security requirements than the default requirements can be provided with the tool.

7 Acknowledgments

Many thanks to my thesis supervisor, Jari Hautamäki, for his valuable guidance. I also want to thank all the experts I had the chance to interview. Your feedback on the tool was valuable. Last but not least, I would like to thank my lovely lady for her support.

References

Al-Essa, H., & Al-Sharidah, A. (2018). *An Approach to Automate Business Impact Analysis*. IEEE. https://doi.org/10.1109/SysEng.2018.8544438

Alwi, A., & Ariffin, K. (2018). *Information Security Risk Assessment for the Malaysian Aeronautical Information Management System*. IEEE. https://doi.org/10.1109/CR.2018.8626841

Anang, A., Arfive, G., & Sucahyo, Y. G. (2021). *The Design of Information Security Risk Management: A Case Study Human Resources Information System at XYZ University*. IEEE. https://doi.org/10.1109/IC2IE53219.2021.9649035

ASSA ABLOY. (2020). *Protecting your data against physical threats*. https://www.assaabloy.com/za/en/product-assets/digital-access-solutions-and-access-control/wireless-card-ble-locking-solutions/assets/documents/AA_Aperio_KS100_Whitepaper_05_2020_ENG_EMEA_Screenversion.pdf

Beinschróth, J. (2022). *Implementing an effective qualitative risk analysis*. IEEE. https://doi-org.ezproxy.jamk.fi:2443/10.1109/ICCC202255925.2022.9922899

Boodai, R. M., Alessa, H. A., & Alanazi, A. H. (2022). *An Approach to Address Risk Management Challenges: Focused on IT Governance Framework*. IEEE. https://doi.org/10.1109/CSR54599.2022.9850318

Carvalho, C., & Marques, E. (2019). *Adapting ISO 27001 to a Public Institution*. IEEE. https://doi.org/10.23919/CISTI.2019.8760870

Cyberwatch Finland. (2021). *Digitalisaatioaiheiden ja kyberriskien huomioiminen yrityksien strategioissa*. https://www.digipooli.fi/sites/digipooli/files/inline-files/%23Strategia22_Projektin_Kysely-tutkimuksen_Tutkimusraportti_v1.pdf

DVV. (2021). *Digiturvallisuuden riskikyselyn tuloksia, syksy 2021*. https://dvv.fi/documents/16079645/0/Digiturvallisuuden_riskikyselyn_tulokset_syksy2021.pdf/32f991cd-1b0e-9275-fadb-2d5166c2102c/Digiturvallisuuden_riskikyselyn_tulokset_syksy2021.pdf?t=1639476332261

Eronen, J., & Kelo, T. (2020). *Experiences from Development of Security Audit Criteria.* European Conference on Cyber Warfare and Security. http://jultika.oulu.fi/files/nbnfi-fe2020043023362.pdf

Finance Finland. (2017). *Camera Surveillance Design Guide, K-method*. Finance Finland. https://www.finanssiala.fi/wp-content/uploads/2017/08/Kameravalvonnan_suunnitteluohje_K-menetelma.pdf

Finlex. (2015). *Law on Public Administration Security Network Operations*. Edita Publishing Oy. https://www.finlex.fi/fi/laki/ajantasa/2015/20150010

Finlex. (2019). *Decree of the Government on the Security Classification of Documents in the State Administration*. Edita Publishing Oy. https://www.finlex.fi/fi/laki/alkup/2019/20191101#Pidm46651396225472

Finnish Government. (2023). *Finland and Nato*. https://um.fi/finlands-membership-in-nato

Finnish Security and Intelligence. (2024). *What kind of Security Clearance Vetting Does Supo Perform.* Finnish Security and Intelligence. https://supo.fi/en/what-kind-of-security-clearance-vetting-does-supo-perform

Grishaeva, S., & Borzov, V. (2021). *Information Security Risk Management*. IEEE. https://doi.org/10.1109/ITQMIS51053.2020.9322901

Harju, V. (2020). *Access Control in Länsi-Uusimaa Department for Rescue Services: Updating the Guidelines and Procedures*. Laurea University of Applied Sciences. https://urn.fi/URN:NBN:fi:amk-2020061518695

Helsinki City Rescue Services. (2022a). *Rescue stations*. https://pelastustoimi.fi/en/helsinki/about-us/rescue-stations

Helsinki City Rescue Services. (2022b). *Helsingin kaupungin pelastuslaitoksen strategia 2022–2025*. https://pelastustoimi.fi/documents/25266713/155701668/Pelastuslaitoksen+strategia+2022-2025.pdf

Helsinki City Rescue Services. (2024). *Helsinki City Rescue Services Duty and Organisation*. https://pelastustoimi.fi/en/helsinki/about-us/duty-and-organisation

Hewitt, J., & Pham, J. (2018). *Qualitative Versus Quantitative Methods in Safety Risk Management*. IEEE. https://doi.org/10.1109/RAM.2018.8463052

ISO/IEC 22301. (2019). *Security and Resilience. Business Continuity Management Systems. Requirements (ISO 22301:2019).* Finnish Standards Association SFS.

ISO/IEC 27000. (2022). *ISO/IEC 27000 Family. Information Security Management*. ISO/IEC 27000. https://www.iso.org/standard/iso-iec-27000-family

ISO/IEC 27001. (2022). *Information Security, Cybersecurity and Privacy Protection. Information Security Management Systems. Requirements (ISO/IEC 27001:2022)*. Finnish Standards Association SFS.

ISO/IEC 27002. (2022). *Information Security, Cybersecurity and Privacy Protection. Information Security Controls (ISO/IEC 27002:2022)*. Finnish Standards Association SFS.

ISO/IEC 27005. (2022). *Information Security, Cybersecurity and Privacy protection. Guidance on Managing Information Security Risks (ISO/IEC 27005:2022)*. Finnish Standards Association SFS.

Jamk University of Applied Sciences. (2024). *Ethical Principles*. https://www.jamk.fi/en/media/41333

Kaipainen, L. (2015). *Information Security Practices for Rescue Departments. Laurea University of Applied Sciences*. https://urn.fi/URN:NBN:fi:amk-201502041891

Kananen, Jorma. (2017). *Laadullinen tutkimus pro graduna ja opinnäytetyönä*. JAMK.

Kusprasapta, M., & Putra, I. M. M. (2021). *Designing Information Security Risk Management on Bali Regional Police Command Center Based on ISO 27005*. IEEE. https://doi.org/10.1109/EIConCIT50028.2021.9431865

NSA. (2020). *Katakri 2020*. Traficom publication series. https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf/ab9c2d4a-5031-3670-6743-3f8921dce8c9?t=1608302599246

NSA. (2023). *Katakri 2020 Liite IV: Naton turvallisuusluokitellun tiedon suojaaminen*. Traficom publication series. https://um.fi/documents/35732/0/Katakri-2020-Liite-IV-2023-05-10+%282%29.pdf/44c7c71b-00ad-151d-080f-fb40a70b5fa3?t=1683795318174

Organisation Chart. (2024). Social Services, Health Care and Rescue Services Division Organisation 2024. https://www.hel.fi/static/sotepe/organisaatiokaaviot/Sotepe-toimiala_2024_fi-sv-en.pdf

Patiño, S., Solís, E., Yoo, S., & Arroyo, R. (2018). *ICT Risk Management Methodology Proposal for Governmental Entities Based on ISO/IEC 27005*. IEEE. https://doi.org/10.1109/ICEDEG.2018.8372361

Pietrzak, M., & Paliszkiewicz, J. (2015). *Framework of Strategic Learning: The PDCA Cycle. Warsaw University of Life Sciences*. https://www.fm-kp.si/zalozba/ISSN/1854-4231/10_149-161.pdf

Pukki, T. (2022). *Security Audit and Development for the Volunteer Fire Departments, That Operate Under Kymenlaakso Rescue Department's Southern Operational Sector*. South-Eastern Finland University of Applied Sciences. https://urn.fi/URN:NBN:fi:amk-2022121228111

Putra, S., Gunawan, M., Sobri, A., Muslimin, JM., Amilin, & Saepudin, D. (2020). *Information Security Risk Management Analysis Using ISO 27005: 2011 For the Telecommunication Company*. IEEE. https://doi.org/10.1109/CITSM50537.2020.9268845

Quinn, S., Ivy, N., Chua, J., Barrett, M., Feldman, L., Topper, D., Witte, G., Gardner, R. K., s& Scarfone, K. (2023). *Enterprise Impact of Information and Communications Technology Risk*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-221

Rajamäki, J. (2015). *Utilization of the Finnish National Security Auditing Criteria "KATAKRI" in the EU FP7 PERSEUS project*. International Journal of Computers and Communications. https://www.naun.org/main/UPress/cc/2015/a202012-142.pdf

Ross, R., Pillitteri, V., Dempsey, K., Riddle, M., & Guissanie, G. (2020). *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-171r2

Savolainen, T. (2023). *A Safe Learning Environment from the Perspective of Laurea University of Applied Sciences Safety, Security and Risk Management Students and Staff*. ScienceDirect. https://doi.org/10.1016/j.heliyon.2023.e12836

Sedinić, I., & Perušić, T. (2015). *Security Risk Management in Complex Organization*. IEEE. https://doi.org/10.1109/MIPRO.2015.7160481

Stefanova-Stoyanova, V., & Danov, P. (2022). *Comparative Analysis of Specialized Standards and Methods on Increasing the Effectiveness and Role of PDCA for Risk Control in Management Systems*. IEEE. https://doi.org/10.1109/COMSCI55378.2022.9912583

Sun, Z., Zhang, J., Yang, H., & Li, J. (2020). *Research on the Effectiveness Analysis of Information Security Controls*. IEEE. https://doi.org/10.1109/ITNEC48623.2020.9084809

Syri, Minna. (2016). *Developing a Tool for Improving an Organization's Premises Security*. Laurea University of Applied Sciences. https://urn.fi/URN:NBN:fi:amk-2016111816511

Tsochev, G., & Stankov, I. (2020). *A Study on Information Security Management*. IEEE. https://doi.org/10.1109/ET50336.2020.9238331

Valtiovarainministeriö. (2013). *Toimitilojen tietoturvaohje*. https://finlex.fi/data/normit/41654/Toimitilojen_tietoturvaohje_VAHTI_2_2013_netti.pdf

Valtiovarainministeriö. (2023). *Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri)*. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/165015/VM_2023_46_Julkri.pdf?sequence=1&isAllowed=y

Velasco, J., Ullauri, R., Pilicita, L., Jácome, B., Saa, P., & Moscoso-Zea, O. (2018). *Benefits of Implementing an ISMS According to the ISO 27001 Standard in the Ecuadorian Manufacturing Industry*. IEEE. https://doi.org/10.1109/INCISCOS.2018.00049

Zhang, X., & He, Y. (2021). *Information Security Management based on Risk Assessment and Analysis*. IEEE. https://doi.org/10.1109/ICISCE50968.2020.00159

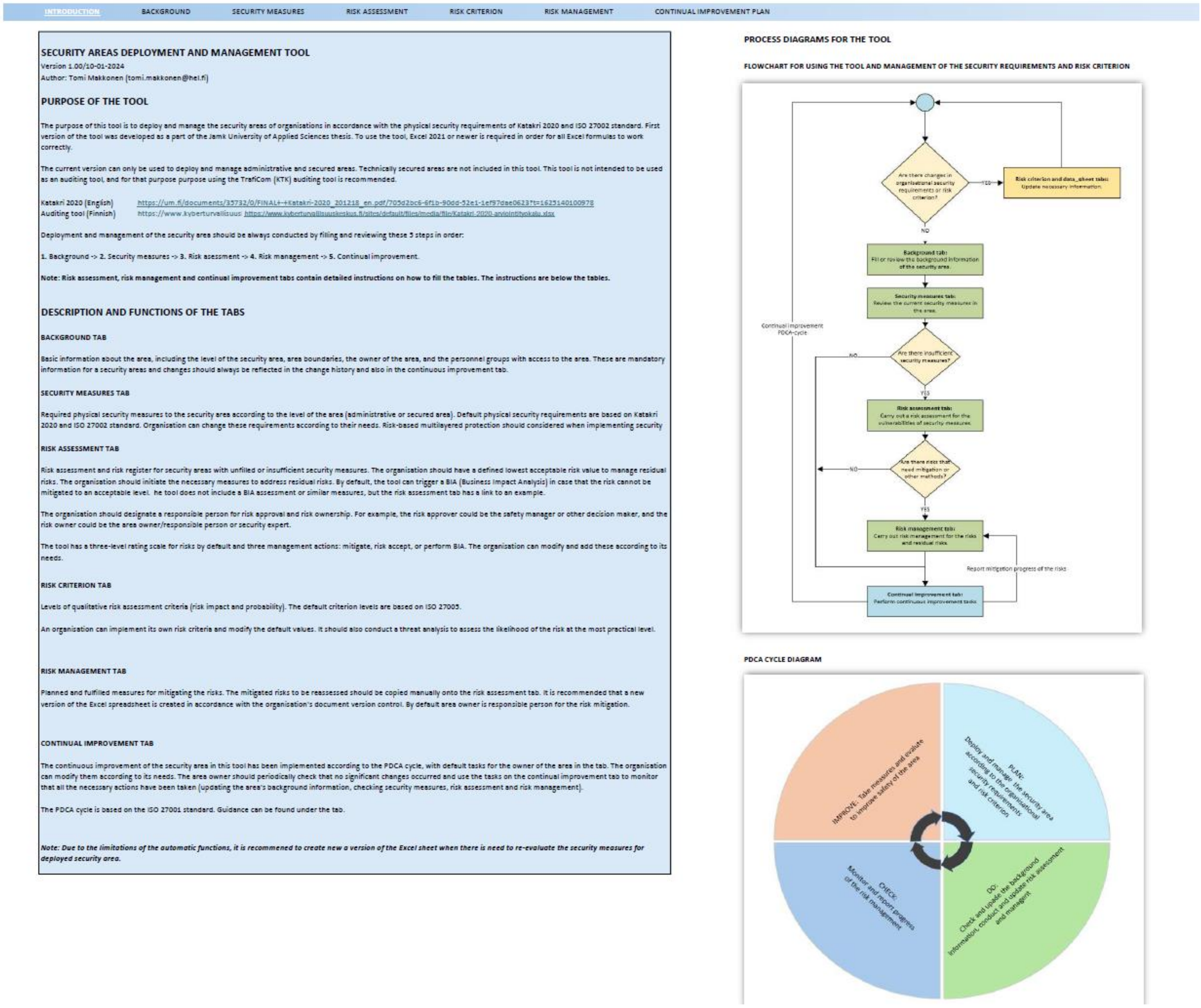
Appendices

Appendix 1. Interview Questions

1. Is a qualitative risk assessment an adequate method for this tool, which is intended to be used by the area owner and security experts?
2. Is the default three-level rating scale appropriate for the risk assessment used in the tool or can it be implemented in another way?
3. Are the current fields in the risk assessment table sufficient or should more be added?
4. Are the current risk management measures sufficient in risk assessment or should there be more options?
5. Would the default set of risk criteria that comes with the tool be sufficient to get your organisation started with risk assessment?
6. The tool includes field for the level of risk acceptance by the organisation and calls for a separate BIA process in case that the risk is not acceptable after mitigation. Is this useful to bring up in the tool?
7. How could the tool's risk assessment process be further developed as a whole?
8. Has the risk management tab brought up all the necessary fields required for risk management?
9. Do you have any ideas for further development of the risk management in the tool?
10. Do you have any ideas on how to improve the versioning of the documents produced by the tool? Now users must manually create a new Excel-sheet of the tool if the security measures for a site need to be reassessed.
11. For continuous improvement, the tool has default tasks that should always be performed according to the PDCA cycle. Do you think the PDCA cycle works in this kind of tool?
12. What is clear and what is unclear about the tasks?
13. As an example, the tool provides four action points where continuous improvement should be triggered. What other action points could be added, for example for organisations?
14. How could the tool's continuous improvement be further developed?
15. Do you find this cross-functional tool useful for the management and deployment of security areas?

Appendix 2. A Populated Example of the Tool

Introduction tab



SECURITY AREAS DEPLOYMENT AND MANAGEMENT TOOL
Version 1.00/10-01-2024
Author: Tomi Makkonen (tomi.makkonen@hel.fi)

PURPOSE OF THE TOOL

The purpose of this tool is to deploy and manage the security areas of organisations in accordance with the physical security requirements of Katakri 2020 and ISO 27002 standard. First version of the tool was developed as a part of the Jamk University of Applied Sciences thesis. To use the tool, Excel 2021 or newer is required in order for all Excel formulas to work correctly.

The current version can only be used to deploy and manage administrative and secured areas. Technically secured areas are not included in this tool. This tool is not intended to be used as an auditing tool, and for that purpose purpose using the TrafiCom (KTK) auditing tool is recommended.

Katakri 2020 (English)	https://um.fi/documents/35732/0/FINAL+-+Katakri-2020_201218_en.pdf/705d2bc6-6f1b-90dd-52e1-1ef97dae0623?t=1625140100978
Auditing tool (Finnish)	https://www.kyberturvallisuus https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Katakri-2020-arviointityokalu.xlsx

Deployment and management of the security area should be always conducted by filling and reviewing these 5 steps in order:

1. Background -> 2. Security measures -> 3. Risk asessment -> 4. Risk management -> 5. Continual improvement.

Note: Risk assessment, risk management and continual improvement tabs contain detailed instructions on how to fill the tables. The instructions are below the tables.

DESCRIPTION AND FUNCTIONS OF THE TABS

BACKGROUND TAB

Basic information about the area, including the level of the security area, area boundaries, the owner of the area, and the personnel groups with access to the area. These are mandatory information for a security areas and changes should always be reflected in the change history and also in the continuous improvement tab.

SECURITY MEASURES TAB

Required physical security measures to the security area according to the level of the area (administrative or secured area). Default physical security requirements are based on Katakri 2020 and ISO 27002 standard. Organisation can change these requirements according to their needs. Risk-based multilayered protection should considered when implementing security

RISK ASSESSMENT TAB

Risk assessment and risk register for security areas with unfilled or insufficient security measures. The organisation should have a defined lowest acceptable risk value to manage residual risks. The organisation should initiate the necessary measures to address residual risks. By default, the tool can trigger a BIA (Business Impact Analysis) in case that the risk cannot be mitigated to an acceptable level. he tool does not include a BIA assessment or similar measures, but the risk assessment tab has a link to an example.

The organisation should designate a responsible person for risk approval and risk ownership. For example, the risk approver could be the safety manager or other decision maker, and the risk owner could be the area owner/responsible person or security expert.

The tool has a three-level rating scale for risks by default and three management actions: mitigate, risk accept, or perform BIA. The organisation can modify and add these according to its needs.

RISK CRITERION TAB

Levels of qualitative risk assessment criteria (risk impact and probability). The default criterion levels are based on ISO 27005.

An organisation can implement its own risk criteria and modify the default values. It should also conduct a threat analysis to assess the likelihood of the risk at the most practical level.

RISK MANAGEMENT TAB

Planned and fulfilled measures for mitigating the risks. The mitigated risks to be reassessed should be copied manually onto the risk assessment tab. It is recommended that a new version of the Excel spreadsheet is created in accordance with the organisation's document version control. By default area owner is responsible person for the risk mitigation.

CONTINUAL IMPROVEMENT TAB

The continuous improvement of the security area in this tool has been implemented according to the PDCA cycle, with default tasks for the owner of the area in the tab. The organisation can modify them according to its needs. The area owner should periodically check that no significant changes occurred and use the tasks on the continual improvement tab to monitor that all the necessary actions have been taken (updating the area's background information, checking security measures, risk assessment and risk management).

The PDCA cycle is based on the ISO 27001 standard. Guidance can be found under the tab.

Note: Due to the limitations of the automatic functions, it is recommened to create new a version of the Excel sheet when there is need to re-evaluate the security measures for deployed security area.

PROCESS DIAGRAMS FOR THE TOOL

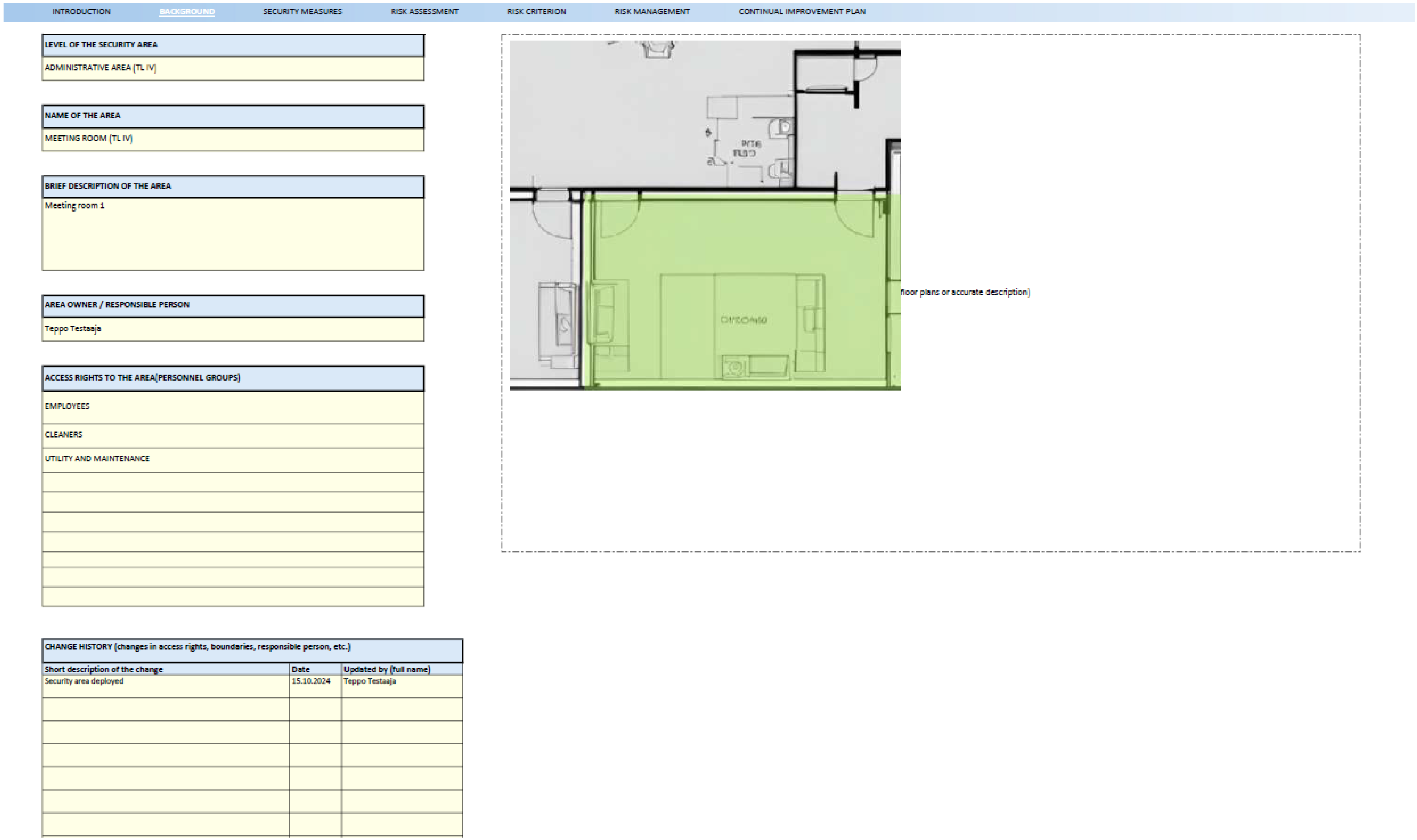
FLOWCHART FOR USING THE TOOL AND MANAGEMENT OF THE SECURITY REQUIREMENTS AND RISK CRITERION

Are there changes in organizational security requirements or risk criterion?
YES
Risk criterion and data_sheet tabs: Update necessary information.
NO
Background tab: Fill or review the background information of the security area.
Security measures tab: Review the current security measures in the area.
Continual improvement PDCA-cycle
Are there insufficient security measures?
NO
YES
Risk assessment tab: Carry out a risk assessment for the vulnerabilities of security measures.
Are there risks that need mitigation or other methods?
NO
YES
Risk management tab: Carry out risk management for the risks and residual risks.
Report mitigation progress of the risks
Continual improvement tab: Perform continuous improvement tasks.

PDCA CYCLE DIAGRAM

PLAN: Deploy and manage the security area according to the organisational security requirements and risk criterion
DO: Check and upade the background information, conduct and update risk assessment and managemt
CHECK: Monitor and report progress of the risk management
IMPROVE: Take measures and evalute to improve safety of the area

Background tab



LEVEL OF THE SECURITY AREA
ADMINISTRATIVE AREA (TL IV)

NAME OF THE AREA
MEETING ROOM (TL IV)

BRIEF DESCRIPTION OF THE AREA
Meeting room 1

AREA OWNER / RESPONSIBLE PERSON
Teppo Testaaja

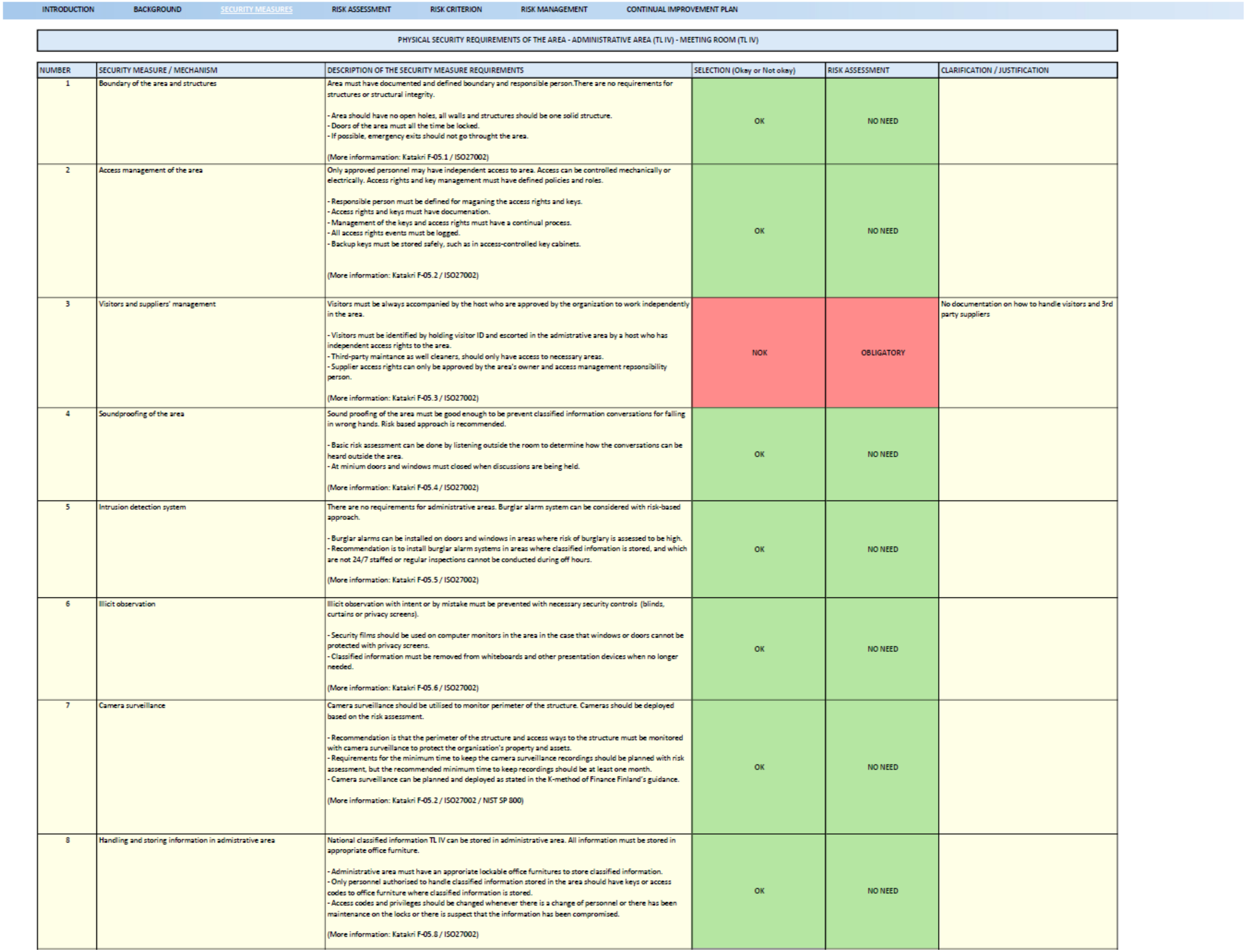
ACCESS RIGHTS TO THE AREA(PERSONNEL GROUPS)
EMPLOYEES
CLEANERS
UTILITY AND MAINTENANCE

floor plans or accurate description)

CHANGE HISTORY (changes in access rights, boundaries, responsible person, etc.)

Short description of the change	Date	Updated by (full name)
Security area deployed	15.10.2024	Teppo Testaaja

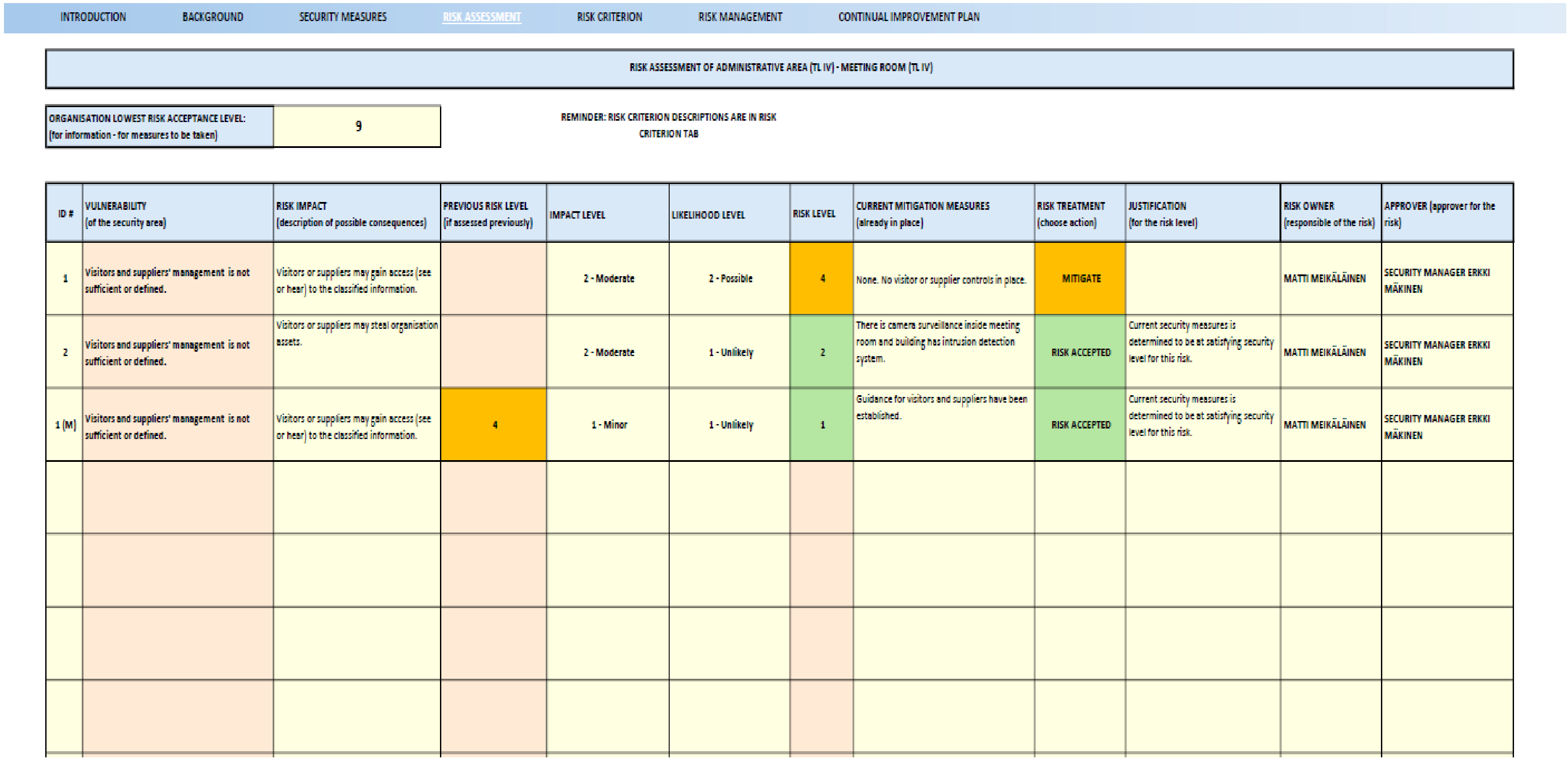
Security measures tab



PHYSICAL SECURITY REQUIREMENTS OF THE AREA - ADMINISTRATIVE AREA (TL IV) - MEETING ROOM (TL IV)

NUMBER	SECURITY MEASURE / MECHANISM	DESCRIPTION OF THE SECURITY MEASURE REQUIREMENTS	SELECTION (Okay or Not okay)	RISK ASSESSMENT	CLARIFICATION / JUSTIFICATION
1	Boundary of the area and structures	Area must have documented and defined boundary and responsible person.There are no requirements for structures or structural integrity. - Area should have no open holes, all walls and structures should be one solid structure. - Doors of the area must all the time be locked. - If possible, emergency exits should not go throught the area. (More informamation: Katakri F-05.1 / ISO27002)	OK	NO NEED	
2	Access management of the area	Only approved personnel may have independent access to area. Access can be controlled mechanically or electrically. Access rights and key management must have defined policies and roles. - Responsible person must be defined for maganing the access rights and keys. - Access rights and keys must have documenation. - Management of the keys and access rights must have a continual process. - All access rights events must be logged. - Backup keys must be stored safely, such as in access-controlled key cabinets. (More information: Katakri F-05.2 / ISO27002)	OK	NO NEED	
3	Visitors and suppliers' management	Visitors must be always accompanied by the host who are approved by the organization to work independently in the area. - Visitors must be identified by holding visitor ID and escorted in the admistrative area by a host who has independent access rights to the area. - Third-party maintance as well cleaners, should only have access to necessary areas. - Supplier access rights can only be approved by the area's owner and access management repsonsibility person. (More information: Katakri F-05.3 / ISO27002)	NOK	OBLIGATORY	No documentation on how to handle visitors and 3rd party suppliers
4	Soundproofing of the area	Sound proofing of the area must be good enough to be prevent classified information conversations for falling in wrong hands. Risk based approach is recommended. - Basic risk assessment can be done by listening outside the room to determine how the conversations can be heard outside the area. - At minium doors and windows must closed when discussions are being held. (More information: Katakri F-05.4 / ISO27002)	OK	NO NEED	
5	Intrusion detection system	There are no requirements for administrative areas. Burglar alarm system can be considered with risk-based approach. - Burglar alarms can be installed on doors and windows in areas where risk of burglary is assessed to be high. - Recommendation is to install burglar alarm systems in areas where classified infomation is stored, and which are not 24/7 staffed or regular inspections cannot be conducted during off hours. (More information: Katakri F-05.5 / ISO27002)	OK	NO NEED	
6	Illicit observation	Illicit observation with intent or by mistake must be prevented with necessary security controls (blinds, curtains or privacy screens). - Security films should be used on computer monitors in the area in the case that windows or doors cannot be protected with privacy screens. - Classified information must be removed from whiteboards and other presentation devices when no longer needed. (More information: Katakri F-05.6 / ISO27002)	OK	NO NEED	
7	Camera surveillance	Camera surveillance should be utilised to monitor perimeter of the structure. Cameras should be deployed based on the risk assessment. - Recommendation is that the perimeter of the structure and access ways to the structure must be monitored with camera surveillance to protect the organisation's property and assets. - Requirements for the minimum time to keep the camera surveillance recordings should be planned with risk assessment, but the recommended minimum time to keep recordings should be at least one month. - Camera surveillance can be planned and deployed as stated in the K-method of Finance Finland's guidance. (More information: Katakri F-05.2 / ISO27002 / NIST SP 800)	OK	NO NEED	
8	Handling and storing information in admistrative area	National classified information TL IV can be stored in administrative area. All information must be stored in appropriate office furniture. - Administrative area must have an approriate lockable office furnitures to store classified information. - Only personnel authorised to handle classified information stored in the area should have keys or access codes to office furniture where classified information is stored. - Access codes and privileges should be changed whenever there is a change of personnel or there has been maintenance on the locks or there is suspect that the information has been compromised. (More information: Katakri F-05.8 / ISO27002)	OK	NO NEED	

Risk assessment tab



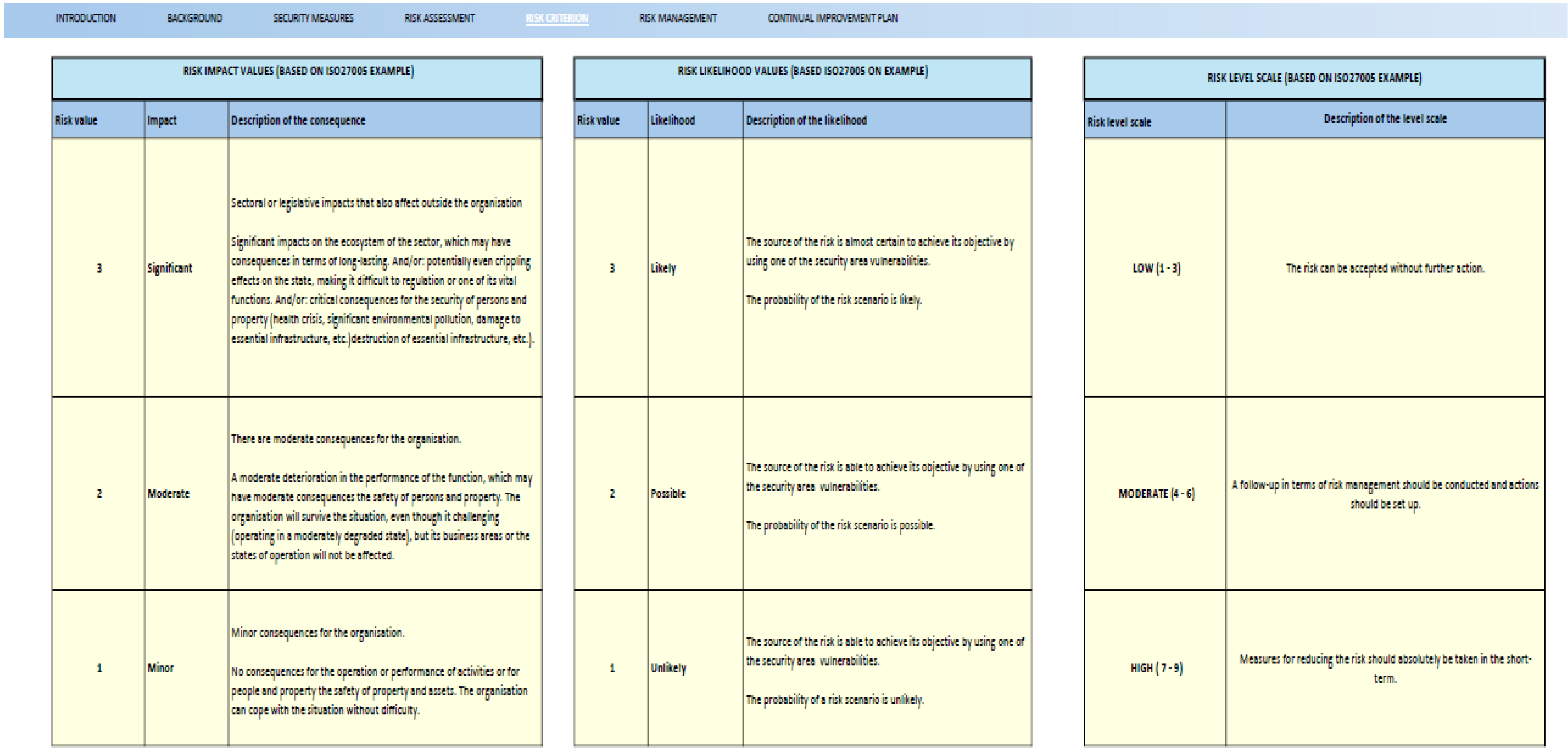
RISK ASSESSMENT OF ADMINISTRATIVE AREA (TL IV) - MEETING ROOM (TL IV)

ORGANISATION LOWEST RISK ACCEPTANCE LEVEL: (for information - for measures to be taken)	9

REMINDER: RISK CRITERION DESCRIPTIONS ARE IN RISK CRITERION TAB

ID #	VULNERABILITY (of the security area)	RISK IMPACT (description of possible consequences)	PREVIOUS RISK LEVEL (if assessed previously)	IMPACT LEVEL	LIKELIHOOD LEVEL	RISK LEVEL	CURRENT MITIGATION MEASURES (already in place)	RISK TREATMENT (choose action)	JUSTIFICATION (for the risk level)	RISK OWNER (responsible of the risk)	APPROVER (approver for the risk)
1	Visitors and suppliers' management is not sufficient or defined.	Visitors or suppliers may gain access (see or hear) to the classified information.		2 - Moderate	2 - Possible	4	None. No visitor or supplier controls in place.	MITIGATE		MATTI MEIKÄLÄINEN	SECURITY MANAGER ERKKI MÄKINEN
2	Visitors and suppliers' management is not sufficient or defined.	Visitors or suppliers may steal organisation assets.		2 - Moderate	1 - Unlikely	2	There is camera surveillance inside meeting room and building has intrusion detection system.	RISK ACCEPTED	Current security measures is determined to be at satisfying security level for this risk.	MATTI MEIKÄLÄINEN	SECURITY MANAGER ERKKI MÄKINEN
1 (M)	Visitors and suppliers' management is not sufficient or defined.	Visitors or suppliers may gain access (see or hear) to the classified information.	4	1 - Minor	1 - Unlikely	1	Guidance for visitors and suppliers have been established.	RISK ACCEPTED	Current security measures is determined to be at satisfying security level for this risk.	MATTI MEIKÄLÄINEN	SECURITY MANAGER ERKKI MÄKINEN

Risk criterion tab



RISK IMPACT VALUES (BASED ON ISO27005 EXAMPLE)

Risk value	Impact	Description of the consequence
3	Significant	Sectoral or legislative impacts that also affect outside the organisation Significant impacts on the ecosystem of the sector, which may have consequences in terms of long-lasting. And/or: potentially even crippling effects on the state, making it difficult to regulation or one of its vital functions. And/or: critical consequences for the security of persons and property (health crisis, significant environmental pollution, damage to essential infrastructure, etc.)destruction of essential infrastructure, etc.).
2	Moderate	There are moderate consequences for the organisation. A moderate deterioration in the performance of the function, which may have moderate consequences the safety of persons and property. The organisation will survive the situation, even though it challenging (operating in a moderately degraded state), but its business areas or the states of operation will not be affected.
1	Minor	Minor consequences for the organisation. No consequences for the operation or performance of activities or for people and property the safety of property and assets. The organisation can cope with the situation without difficulty.

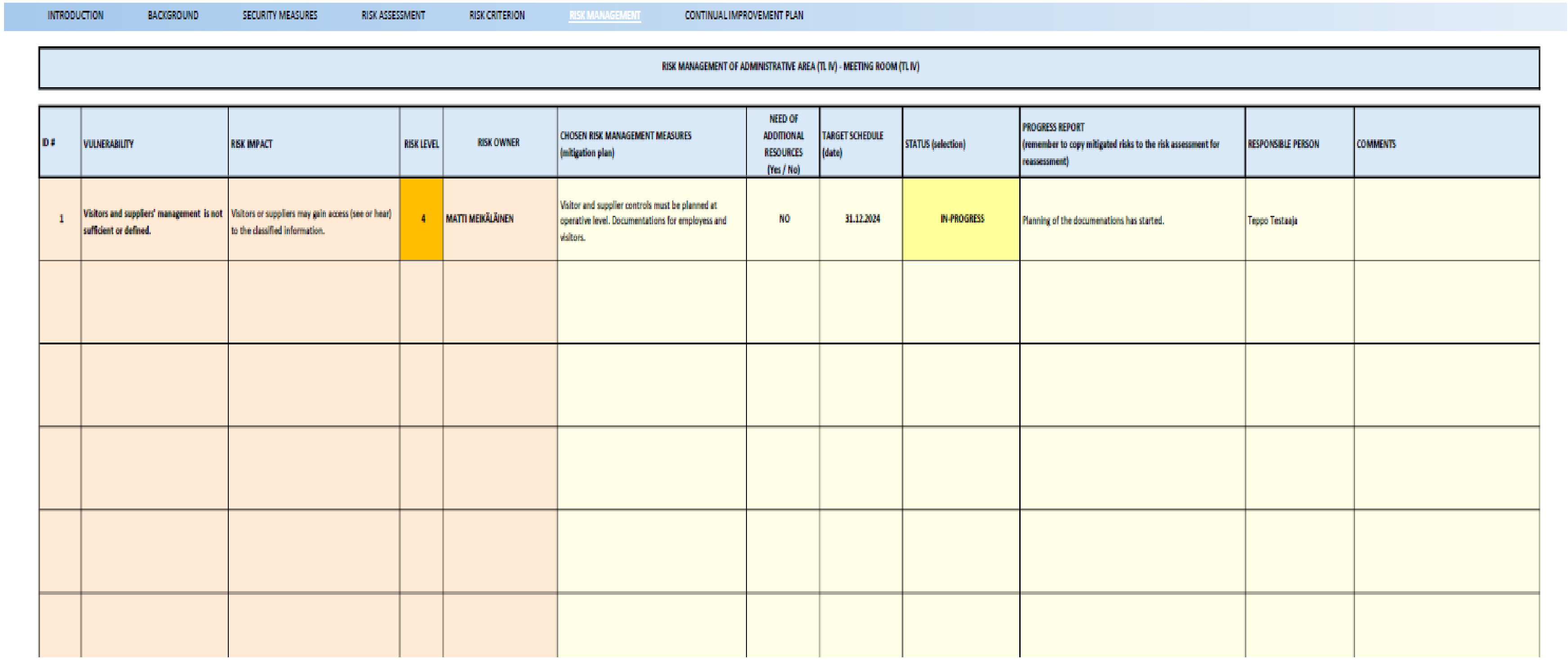
RISK LIKELIHOOD VALUES (BASED ISO27005 ON EXAMPLE)

Risk value	Likelihood	Description of the likelihood
3	Likely	The source of the risk is almost certain to achieve its objective by using one of the security area vulnerabilities. The probability of the risk scenario is likely.
2	Possible	The source of the risk is able to achieve its objective by using one of the security area vulnerabilities. The probability of the risk scenario is possible.
1	Unlikely	The source of the risk is able to achieve its objective by using one of the security area vulnerabilities. The probability of a risk scenario is unlikely.

RISK LEVEL SCALE (BASED ON ISO27005 EXAMPLE)

Risk level scale	Description of the level scale
LOW (1 - 3)	The risk can be accepted without further action.
MODERATE (4 - 6)	A follow-up in terms of risk management should be conducted and actions should be set up.
HIGH (7 - 9)	Measures for reducing the risk should absolutely be taken in the short-term.

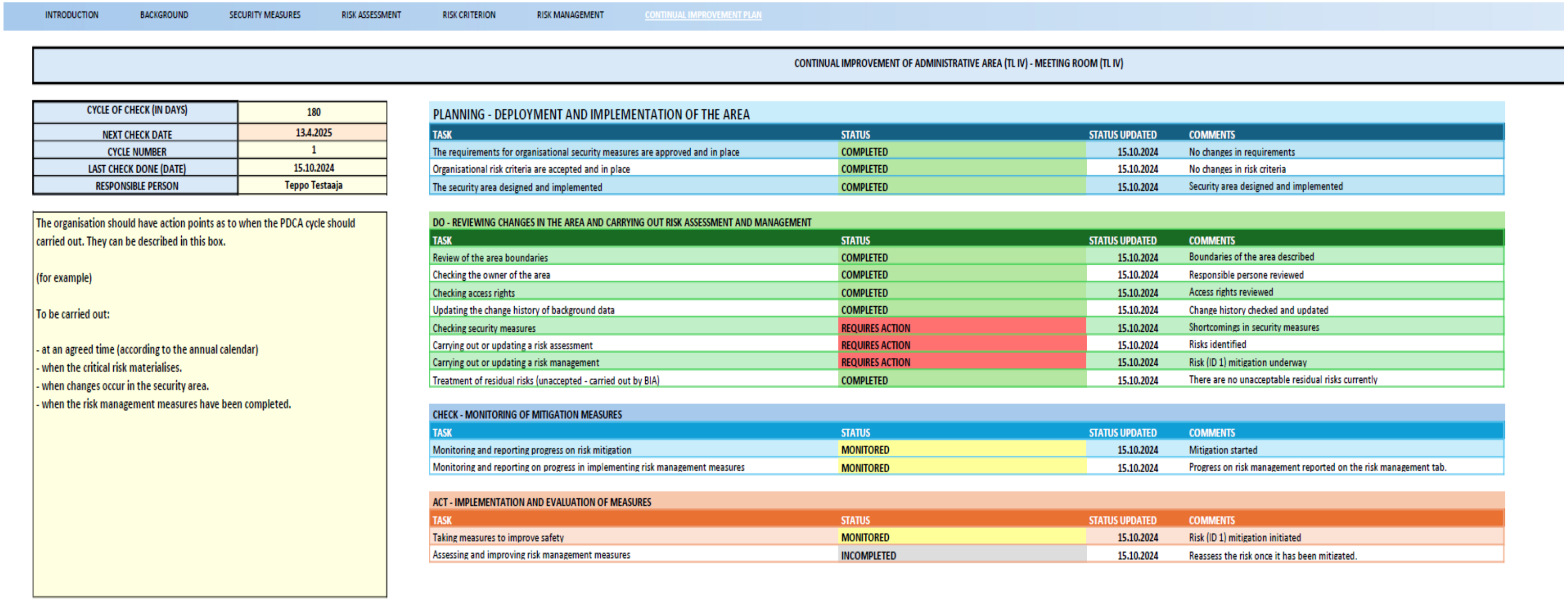
Risk management tab



RISK MANAGEMENT OF ADMINISTRATIVE AREA (TL IV) - MEETING ROOM (TL IV)

ID #	VULNERABILITY	RISK IMPACT	RISK LEVEL	RISK OWNER	CHOSEN RISK MANAGEMENT MEASURES (mitigation plan)	NEED OF ADDITIONAL RESOURCES (Yes / No)	TARGET SCHEDULE (date)	STATUS (selection)	PROGRESS REPORT (remember to copy mitigated risks to the risk assessment for reassessment)	RESPONSIBLE PERSON	COMMENTS
1	Visitors and suppliers' management is not sufficient or defined.	Visitors or suppliers may gain access (see or hear) to the classified information.	4	MATTI MEIKÄLÄINEN	Visitor and supplier controls must be planned at operative level. Documentations for employess and visitors.	NO	31.12.2024	IN-PROGRESS	Planning of the documenations has started.	Teppo Testaaja	

Continual improvement tab



CONTINUAL IMPROVEMENT OF ADMINISTRATIVE AREA (TL IV) - MEETING ROOM (TL IV)

CYCLE OF CHECK (IN DAYS)	180
NEXT CHECK DATE	13.4.2025
CYCLE NUMBER	1
LAST CHECK DONE (DATE)	15.10.2024
RESPONSIBLE PERSON	Teppo Testaaja

The organisation should have action points as to when the PDCA cycle should carried out. They can be described in this box.

(for example)

To be carried out:

- at an agreed time (according to the annual calendar)
- when the critical risk materialises.
- when changes occur in the security area.
- when the risk management measures have been completed.

PLANNING - DEPLOYMENT AND IMPLEMENTATION OF THE AREA

TASK	STATUS	STATUS UPDATED	COMMENTS
The requirements for organisational security measures are approved and in place	COMPLETED	15.10.2024	No changes in requirements
Organisational risk criteria are accepted and in place	COMPLETED	15.10.2024	No changes in risk criteria
The security area designed and implemented	COMPLETED	15.10.2024	Security area designed and implemented

DO - REVIEWING CHANGES IN THE AREA AND CARRYING OUT RISK ASSESSMENT AND MANAGEMENT

TASK	STATUS	STATUS UPDATED	COMMENTS
Review of the area boundaries	COMPLETED	15.10.2024	Boundaries of the area described
Checking the owner of the area	COMPLETED	15.10.2024	Responsible persone reviewed
Checking access rights	COMPLETED	15.10.2024	Access rights reviewed
Updating the change history of background data	COMPLETED	15.10.2024	Change history checked and updated
Checking security measures	REQUIRES ACTION	15.10.2024	Shortcomings in security measures
Carrying out or updating a risk assessment	REQUIRES ACTION	15.10.2024	Risks identified
Carrying out or updating a risk management	REQUIRES ACTION	15.10.2024	Risk (ID 1) mitigation underway
Treatment of residual risks (unaccepted - carried out by BIA)	COMPLETED	15.10.2024	There are no unacceptable residual risks currently

CHECK - MONITORING OF MITIGATION MEASURES

TASK	STATUS	STATUS UPDATED	COMMENTS
Monitoring and reporting progress on risk mitigation	MONITORED	15.10.2024	Mitigation started
Monitoring and reporting on progress in implementing risk management measures	MONITORED	15.10.2024	Progress on risk management reported on the risk management tab.

ACT - IMPLEMENTATION AND EVALUATION OF MEASURES

TASK	STATUS	STATUS UPDATED	COMMENTS
Taking measures to improve safety	MONITORED	15.10.2024	Risk (ID 1) mitigation initiated
Assessing and improving risk management measures	INCOMPLETED	15.10.2024	Reassess the risk once it has been mitigated.