jamk

Defining Lean ISMS processes

Case Fimlab

Ville Karuaho

Master’s thesis
05/2024
Master's Degree Programme in Information Technology, Cyber Security (YAMK)

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Description

Karuaho, Ville

Defining Lean ISMS processes, Case Fimlab

Jyväskylä: Jamk University of Applied Sciences, May 2024, 90 pages

Master's Degree Programme in Information Technology, Cyber Security (YAMK). Masters' thesis.

Permission for open access publication: Yes

Language of publication: English

Abstract

A study was conducted to investigate case organizations controls and processes for Lean process optimization. The case organization was going through major ICT transformation project which caused the need to examine the existing cybersecurity controls and assess if further optimization was needed. The objective of this research encompassed several key areas. Firstly, the target was to identify and evaluate the processes within the Information Security Management System (ISMS) of the case organization, with a specific focus on determining areas requiring improvement to enhance cybersecurity. Secondly, the research aimed to identify and analyze the specific problem points within these ISMS processes, establishing opportunities for process optimization. Thirdly, the study sought to explore the application of Lean thinking principles to the ISMS processes, investigating methods to streamline operations and improve efficiency. Finally, the objective was to develop actionable strategies for the implementation of these lean thinking methodologies within the ISMS processes, providing possible solutions to identified issues and the overall improvement for selected cybersecurity processes. The constructive research approach employed mixed methods, combining qualitative and quantitative techniques to gather and analyze data. Applied PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework provided a structure to conduct a systematic review of existing literature. Stakeholder workshop interviews were conducted to gather data from key individuals within the organization. Qualitative data obtained from these interviews was quantified using a developed coding scheme, allowing for systematic analysis and interpretation of the workshop data. Finally, a value stream mapping technique was utilized to visualize and analyze the end-to-end processes related to the Information Security Management System (ISMS) within the organization. By applying mixed methods in the research approach, the research was able to triangulate data from multiple sources. The study successfully identified a category of controls and processes requiring optimization related to information security threats faced in the case organization. The research was able to apply several key Lean thinking principles to the selected processes, aiming to enhance efficiency, streamline operations, and improve cybersecurity threat mitigation efficiency. Based on the findings, it can be concluded that process optimization utilizing lean techniques presents a viable solution for enhancing efficiency and effectiveness in addressing information security challenges within the case organization.

Keywords/tags (subjects)

Cybersecurity, Healthcare, Lean methods, Process analysis

Miscellaneous (Confidential information)

N/A

jamk

Description

Karuaho, Ville

Lean ISMS prosessien määrittely, Case Fimlab

Jyväskylä: Jyväskylän ammattikorkeakoulu, Toukokuu 2024, 90 sivua

Master's Degree Programme in Information Technology, Cyber Security (YAMK). Opinnäytetyö YAMK.

Verkkojulkaisulupa myönnetty: Kyllä

Julkaisun kieli: Englanti

Tiivistelmä

Tutkimus suoritettiin, jotta voitiin selvittää tapausorganisaation kontrolleja sekä prosesseja Lean-prosessioptimoinnin näkökulmasta. Tapausorganisaatio oli läpikäymässä suurta ICT-muutosprojektia, mikä aiheutti tarpeen tutkia olemassa olevia kyberturvallisuuden hallintakeinoja ja arvioida, tarvittiinko lisäoptimointia. Tämän tutkimuksen tavoitteet kattoivat useita keskeisiä alueita. Ensinnäkin pyrittiin tunnistamaan ja arvioimaan tapausorganisaation tietoturvan hallintajärjestelmän (ISMS) prosesseja, kohdistettuna erityisesti parannusta vaativien alueiden kyberturvallisuuden tehostamiseksi. Toiseksi tutkimuksen tavoitteena oli tunnistaa ja analysoida näiden ISMS-prosessien erityiset ongelmakohdat ja luoda mahdollisuuksia prosessien optimoinnille. Kolmanneksi tutkimuksessa pyrittiin tutkimaan Lean-periaatteiden soveltamista ISMS-prosesseihin, selvittäen menetelmiä toimintojen tehostamiseksi ja tehokkuuden parantamiseksi. Lopuksi tavoitteena oli kehittää toimivia strategioita näiden Lean-ajattelumenetelmien soveltamiseksi ISMS-prosesseihin, tarjoten mahdollisia ratkaisuja tunnistettuihin ongelmiin ja yleiseen parannukseen valituissa kyberturvallisuusprosesseissa. Rakentava tutkimuslähestymistapa hyödynsi monimenetelmäisiä tutkimusmenetelmiä, yhdistäen laadullisia ja määrällisiä tapoja tiedon keräämiseksi ja analysoimiseksi. PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) -viitekehystä sovellettiin systemaattisen kirjallisuuskatsauksen suorittamiseen. Tiedon keräämiseksi organisaation avainhenkilöiltä järjestettiin sidosryhmien työpajahaastatteluja. Näistä haastatteluista saatu laadullinen data kvantifioitiin kehitetyn koodausjärjestelmän avulla, mikä mahdollisti työpajadatan systemaattisen analysoinnin ja tulkinnan. Lopuksi käytettiin arvovirtakartoitusmenetelmää ISMS:ään liittyvien prosessien visualisoimiseksi ja analysoimiseksi organisaatiossa. Erilaisia tutkimusmenetelmiä soveltamalla tutkimus pystyi trianguloimaan tietoja useista lähteistä. Tutkimuksessa tunnistettiin onnistuneesti kategoria hallintakeinoja ja prosesseja, jotka vaativat optimointia tapausorganisaation kohtaamien tietoturvauhkien osalta. Tutkimus pystyi soveltamaan useita keskeisiä Lean-ajattelun periaatteita valittuihin prosesseihin, pyrkien tehostamaan toimintaa, virtaviivaistamaan prosesseja ja parantamaan kyberturvauhkiin liittyvää tehokkuutta. Tulosten perusteella voidaan päätellä, että Lean-tekniikoita hyödyntävä prosessien optimointi on varteenotettava ratkaisu tehokkuuden ja vaikuttavuuden parantamiseksi tietoturvahaasteiden käsittelyssä tapausorganisaatiossa.

Avainsanat (asiasanat)

Kyberturvallisuus, Terveydenhuolto, Lean menetelmät, Prosessianalyysi

Muut tiedot (salassa pidettävät liitteet)

N/A

Contents

Figures

Tables

1 Introduction

This chapter will provide background for the thesis research and introduce the commissioner and case organization of the thesis to provide an understanding of the research context. It explores the organizations background and its operations outlining developed systems and work methodologies. It also provides a brief description of the healthcare sector as an IT environment. Furthermore, the background chapter explores the healthcare environment, considering its unique challenges, regulatory frameworks, and cybersecurity considerations. It also delves into fundamental principles such as confidentiality, integrity, and availability from healthcare point of view. Lastly, the chapter discusses the motivation, structure, research approach, and phases of the thesis research.

1.1 Organization

Fimlab is a healthcare company operating in the field of laboratory services, education and research for hospitals, health centers, occupational healthcare, and private customers (Fimlab, 2022). The company offers multiple services for consumers such as diabetes measurement, screening of cervical cancer and intestinal cancer, remote testing of STDs, sampling services including fast blood samples without appointments (Nopsa service). Services also contain infertility treatment, electrocardiography and recently separate Covid testing centers. Results for samples depending on the service and customer location are obtainable via SMS, Fimlab mobile app or in My Kanta Pages (Omakanta). In some cases, results are obtainable through the healthcare organization that has made the referral for the lab tests (Fimlab, 2020-a).

Organizations can make referrals for their patients for laboratory testing. Contractual customers can make orders for sampling materials and packaging and delivery materials for samples. Fimlab can rent point of care analyzers for organizations and offers maintenance and quality assurance for them. Fimlab also offers laboratory services for scientific and clinical research. Services include clinical chemistry, microbiology, pathology, genetics, and pharmacology consultation. Additionally, services include designing, budgeting and agreements for laboratory research packages, guidance and documenting for taking samples and special samples, storage and handling for research samples and handling of samples to be sent elsewhere (Fimlab, 2020-b).

Fimlab started as a small central laboratory for Tampere Central Hospital and grew from there to provide municipal laboratory services for the whole Pirkanmaa. Later it has been joined by Central Finland, Kanta-Häme, Ostrobothnia, and Päijät-Häme regions. Currently it employs approximately 1200 people and server its customers in over 110 locations.

Software development in case organization

In addition to providing laboratory services Fimlab also develops its own Laboratory Information Systems. Currently the organization has X autonomous development teams that provide continuous development for the systems. Software development is done according to SAFe (Scaled Agile Framework) practices. Laboratory systems that Fimlab currently develops are known as WebXLab, Labon, Lab2.0, Omamittaussovellus and Fimlab mobile app. In addition to development teams Fimlab also has IT-infrastructure and networking teams working in synchronization with the development teams in concurrent sprints. The aim of the SAFe model is to synchronize the work of development teams and other teams to bring all development and changes into a more transparent and iterative workflow.

1.2 Healthcare as an environment

Healthcare is a complex and diverse environment. Organizations in the field handle large amounts of sensitive patient data, including personal, medical, and financial information. Data of this type can be highly valuable to cybercriminals, making healthcare a lucrative target for cyberattacks.

The industry relies on technology by a considerable amount to manage and analyze various patient data, from electronic medical records to medical devices connected to the internet. As medical devices and electronic data become increasingly interconnected and used the technology introduces innumerous vulnerabilities for cybercriminals to exploit. These threat actors can exploit vulnerabilities to gain unauthorized access to confidential data or disrupt critical healthcare processes. In their journal article Brody et al. (2018) suggested that malware is not only limited to financial harm, but actual patient lives can be in danger.

Healthcare organizations face regulatory requirements and industry standards that govern the security and privacy of patient data, such as GDPR. In Finland, National Supervisory Authority for Welfare and Health (Valvira) enforces compliance with requirements for systems processing patient data in healthcare services. The requirements vary depending on the classification of the system. The classification of social and healthcare information systems initiates the system's certification and registration process. The system's class significantly influences how its essential requirements are verified. Social and healthcare information systems handling client and patient data are divided into classes A and B. Class A is further divided into subclasses A1, A2, and A3. The classification of the information system is the responsibility of the information system service provider ("National Supervisory Authority for Welfare and Health," n.d.).

1.3 Confidentiality, integrity, and availability

The CIA triad is an abbreviation of the words Confidentiality, Integrity, and Availability. These terms are presented as properties of information and systems to be protected through information security. In a National Institute of Standards and Technology publication, Nieles et al. (2017) define information security as means to protect information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction to ensure the CIA of information is maintained.

Confidentiality involves safeguarding data privacy through access controls, encryption, and multi-factor authentication. (Cawthra et al., 2020) The aim is to restrict access to authorized personnel, preventing both intentional breaches and accidental disclosures. Safeguarding patient confidentiality is paramount in Finland's healthcare sector, as in Europe overall. Data protection laws, including the General Data Protection Regulation (GDPR), enforce the protection of sensitive medical information. (WHO, n.d.)

Data integrity in healthcare ensures the trustworthiness and accuracy of patient information, guarding against tampering. Techniques like hashing, encryption, and digital signatures protect data integrity, while non-repudiation prevents denial of actions, reinforcing trust in data authenticity. (Cawthra et al., 2020) Maintaining the integrity of medical records is vital for safe and effective healthcare. Tampering or unauthorized access to patient records could have serious consequences.

Data availability is essential for organizations and customers, ensuring information accessibility when needed (Cawthra et al., 2020). Despite maintaining confidentiality and integrity, data usability is crucial. Factors like system functionality, network reliability, and timely access are important. Disruptions such as power outages or denial-of-service attacks can compromise availability. Redundant networks, proactive software upgrades, and comprehensive disaster recovery plans enhance availability, ensuring swift recovery after adverse events. In healthcare, availability is important for delivering timely and effective medical care. Any disruption, be it technical failures, natural disasters, or cyberattacks, could affect patient outcomes.

In this thesis research any concept that could harm the confidentiality, integrity and availability of IT-assets is considered a cybersecurity threat. The availability of assets is given a special emphasis through reviewal of major incident reports which are written in result of major incident that results in loss of availability to a service or system.

1.4 Motivation for Thesis

Fimlabs status as a subsidiary of Wellbeing services county of Pirkanmaa (referred later as Pirha, finnish abbreviation from “Pirkanmaan hyvinvointialue”) has changed as the ownership majority is no longer only Pirha but more evenly distributed base of owners coming from Central Finland,

Kanta-Häme, Ostrobothnia, and Päijät-Häme wellbeing services counties (Fimlab, 2023). This indicates that it is no longer favorable for the case organization to be attached to Pirha's IT environment and IT management processes such as change management.

The separation from Pirha networks has launched a massive ICT-transition project. One of the aspects of the transition is to develop cybersecurity processes to replace those that were managed earlier by Pirha. This enables Fimlab to redesign aspects of their processes and streamline them to better serve the whole owner base. In case of cybersecurity, it is obligatory to at least maintain the same level of cybersecurity as it was under Pirha management. This transition servers as an opportunity to revise cybersecurity processes and make effort to improve the overall level of cybersecurity.

1.5 Structure of the thesis

This chapter depicts the structure of the thesis, describing the sequence of topics covered within the document. It begins with the background chapter that provides essential context and background information relevant to the research. Following this, the purpose and objectives of the thesis are described, providing the scope and goals of the study. Next, the literature review section is presented, offering a structured exploration of existing research literature related to the research topic. The process development process is then outlined, detailing the methodology and approach undertaken to address the research questions. The following sections describe the results of the study, followed by conclusions drawn from the findings. Finally, the discussion section contains reflections on the research process, as well as an examination of challenges encountered and potential topics for future research.

1.6 Research approach and methodology

This chapter describes the research approach and various methods used in the thesis research to collect data and analyze it. Based on the objective set for the thesis a constructive research approach for the thesis was chosen.

According to Lukka (2003), constructive research aims to innovate solutions to real world problems and contributes to the theory of the field. The ideal result of a constructive research project

is a solution to the problem provided by a new construction. Construction in Lukka's research is defined as human artefacts: models, diagrams, plans, organization structures, commercial products, and information system designs.

The research methodology utilizes a mixed methods approach, combining qualitative and quantitative techniques to gather and analyze data. Applied PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework provides a structure to conduct a systematic review of existing literature (Prisma 2020 statement, n.d.-a). Stakeholder workshop interviews are used to gather data from key individuals within the organization. Qualitative data obtained from these interviews was quantified using a developed coding scheme, allowing for systematic analysis and interpretation of the workshop data. Finally, a value stream mapping technique is used to visualize and analyze the end-to-end processes related to the cybersecurity processes within the organization. Thesis project is conducted as a research-based development work since the one of the goals of the thesis is to develop existing cybersecurity processes.

By employing constructive approach and mixed methods, the study will be able to triangulate data from multiple sources to provide a comprehensive understanding of the research topic and provide solution to thesis research questions.

1.7 Thesis research phases

The thesis research progresses through several distinct phases aimed at addressing the research questions. Research progress is depicted in Figure 1. It begins with an analysis of security threats sourced from literature review, Security Operation Center (SOC) reports and the major incident calendar. After this, the findings were presented and discussed in collaborative workshops with stakeholders, providing valuable information and perspective on the issue. A valuation framework was developed in which the security threat data was assessed. Similarly workshop stakeholder discussion data was then quantified and analyzed to extract valuation data for the threat categories. This allowed setting valuation values for threat categories and their comparation. After choosing a suitably valuable category the research led to the development of value stream maps, which visualized the current state of security processes and highlighted potential bottlenecks and challenges.

After assessment of the challenges within the processes, future state value streams were proposed to address inefficiencies. These proposed solutions were further refined and validated through additional workshop with stakeholders, ensuring alignment with organizational objectives and goals.

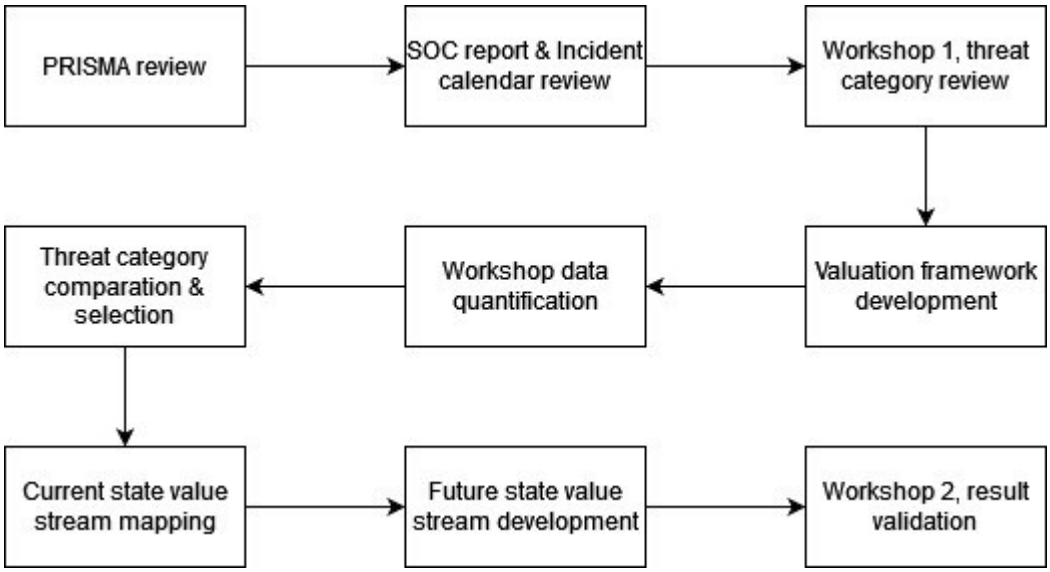

Figure 1. Thesis research phases.

2 Purpose and objective

This chapter describes the purpose and objective of the thesis research. It delves into the reasons behind motivation of the thesis research and outlines the research questions to be answered. Additionally, it visits earlier research performed on the subject and evaluates the significance of the research to be done.

Purpose

The purpose of this thesis is to evaluate the cybersecurity processes within the case organization against the context of a significant ICT transformation. This research aims to analyze the existing cybersecurity control measures, identify strengths, weaknesses, and potential areas for enhancement, and propose strategies to align the organization's security practices with evolving ICT requirements.

Objective and research questions

Objective of the research is to gain answer to research question formulated for this thesis work:

- RQ1: What processes in their Information Security Management System (later abbreviated as ISMS) the case organization should improve to enhance their cybersecurity?
- RQ2: What are the specific problem points that can be solved and improved upon?
- RQ3: How to apply lean thinking to ISMS processes?
- RQ4: How to implement these processes?

These research questions assess the ISMS of the case organization by identifying areas for enhancement and addressing specific problem points. Process improvement is gained by applying lean thinking principles to ISMS processes and developing strategies for implementation. Research aims to accomplish the objectives by identifying valuable cybersecurity threat categories to the case organization, and by gaining verification from the stakeholders. Controls for the threats that are considered to have most impact on organization are assessed. Chosen processes are assessed using Lean methodologies to see if the flow of their value can be accelerated. As an output of this research a Lean cybersecurity process is defined utilizing value stream mapping techniques.

2.1 Review of previous research

In this section, previous research endeavors related to cybersecurity processes in the healthcare sector are explored. Earlier master's and bachelor's thesis works addressing the concepts of safeguarding sensitive information in healthcare and related environment are reviewed and analyzed to provide an understanding of the existing research done in this domain. During the review on previous research on Theseus database several applicable thesis works were identified.

Cybersecurity in healthcare environments

In their respective theses, Suni (2021) and Liesoja (2023) researched specific aspects of cyber security management within the healthcare sector.

In their bachelor's thesis, Suni (2021) researched the development of cyber incident response processes within healthcare environments. The author emphasized the significant need to develop processes and guidelines for managing cyber incidents and disruptions. With medical devices in hospitals frequently connected to the internet and integrated into hospital networks and other devices, the related cybersecurity risks are heightened. Particularly important in healthcare cybersecurity is the sharing of information related to threats, which may involve sharing indicators of compromise (IoCs) or sharing information on vulnerabilities, experiences, and strategies for mitigating disruptions. As a result of the research project, a handbook on cyber incident management for healthcare stakeholders was produced.

In their master's thesis Liesoja (2023) researched cyber security risk management methods tailored specifically for hospital pharmacies. The study focused on identifying cyber security risks inherent in pharmaceutical services, particularly within the context of supply chain structures within hospital pharmacy operations. The study utilized a combination of questionnaires, workshops, and interviews with pharmacy personnel and ICT staff from the case organization in addition to literature review. As a result, the study successfully developed a model for controlling cyber security risks associated with the operations of pharmaceutical services within hospital environment containing defined checklist, process, and monitoring criteria.

Cybersecurity in Municipalities and Subcontracting Chains

In their master's thesis, Pousi (2022) researched municipal cyber security, focusing on understanding the cyber threat landscape faced by municipalities in Finland. The research assessed the level of preparedness of municipalities in safeguarding against potential cyber-attacks. The study, conducted semi-structured thematic interviews with a total of eleven participants, comprising four representatives from municipalities, one from a municipal energy company, five from cybersecurity service providers, and one from the government sector. The study suggested that while has been notable improvement in the technical safeguards implemented by municipalities, there remain disparities in the overall management of cyber security at higher levels. External threats, such as phishing emails targeting sensitive data. The worst-case scenarios generally perceived included the disruption of essential services mandated by law and the malfunctioning of patient information systems within the healthcare sector.

Koskinen (2023) investigated the realization of cybersecurity within subcontracting chains in their master's thesis. The research examined how and why cybersecurity is implemented in subcontracting chains. The study suggested that the widespread use of subcontractors in the IT industry, has a significant impact on overall cybersecurity. Organizations are interdependent in modern society in various ways, and within subcontracting chains, attackers can exploit vulnerabilities in one entity's systems and propagate malware more easily. The research findings highlight the crucial role of management commitment and resource allocation in ensuring cybersecurity within subcontracting chains. Additionally, the importance of expertise, including both technical skills and administrative cybersecurity measures such as company policies and procedures, was emphasized. According to the research cybersecurity is realized when organizations make informed decisions based on well-prepared, understandable, and presented information, in line with the current threat landscape. This requires leadership decisions, commitment, and ongoing monitoring. Key for management is to allocate the necessary resources to enable the implementation of cybersecurity measures effectively.

Conclusion about previous research

Based on these studies it is indicated that effective management of cybersecurity threats involves several key components. These include the sharing of information related to threats among stakeholders, leveraging the expertise and knowledge of key personnel, recognizing the importance of specialized expertise in cybersecurity, and allocating necessary resources to address and mitigate potential threats.

2.2 Significance of research

The research of this thesis aims to integrate Lean (What is lean?, 2023) principles with cybersecurity processes which is a moderately unexplored area of research based on the results of this thesis literature and earlier research review. This research aims to identify most valuable threats related to case organization. Applying Lean methodologies to cybersecurity workflows will generate new knowledge on how cybersecurity processes can be made more efficient. This research provides an example how to assess cybersecurity status of a healthcare laboratory and design effective cybersecurity processes to improve the overall cybersecurity status of the organization by mitigating risks and optimizing processes.

3 Literature review

The chapter outlines the methodology employed in the literature review, including the application of PRISMA systematic review framework (Prisma 2020 statement, n.d.-a). Within this framework, details are provided on screening procedures, eligibility criteria, information sources, search strategy, selection process, data collection, and study characteristics were applied. The chapter then describes the key concepts such as ISMS and Lean methodologies, providing a comprehensive understanding of these foundational theories. Additionally, the chapter examines specific threats to the healthcare sector, identifying the unique challenges faced in this domain. Finally, the chapter contains synthesis on the findings of the literature review, providing observations into existing knowledge gaps and areas of consensus within the academic literature.

3.1 Purpose

The purpose of the literature review is to offer a structured approach to understanding the existing body of knowledge relevant to the research topic (Literature review, 2024). Through systematic examination of academic literature, the review aims to gain knowledge about the thesis. By comprehensively reviewing prior research literature utilizing applied PRISMA review, the review servers to provide insight into theories and concepts related to the research area.

Additionally, the literature review serves as a component of the research methodology. Synthes and analysis of the existing literature aids to establish a theoretical framework and develop research methods and approaches. The literature review step of the research contributes to the validity and credibility of the research process.

3.2 PRISMA systematic review

The PRISMA reporting guideline has been designed primarily for systematic reviews of studies that evaluate the effects of health interventions. However, the PRISMA 2020 statement is designed to be adaptable to systematic reviews covering a range of interventions beyond health, including so-

cial or educational interventions. PRISMA 2020 is suitable for use in systematic reviews that involve synthesis methods, such as meta-analysis, as well as those that do not require synthesis, such as when only one eligible study is identified (Prisma 2020 statement, n.d.-a).

This thesis research systematic review applies PRISMA principles but does not fully commit to the checklist structure (Appendix 1). It applies the principles of eligibility criteria, describing search strategy, describing selection process, and reviewing study characteristics.

3.2.1 Eligibility criteria

During the review process, inclusion and exclusion criteria for the review were formulated. They are presented separately on their respective lists:

1. Inclusion Criteria:
    - Studies that focus on lean ISMS processes.
    - Studies that discuss cybersecurity processes, assessment, or improvement.
    - Studies that address the implementation or formulation of new processes related to cybersecurity.
    - Studies that utilize methodologies such as lean, Cobit 5, NIST CSF, or other relevant frameworks in the context of process improvement.
    - Studies that examine the role of lean principles or agile methodologies in the context of lean ISMS or cybersecurity.
    - Studies conducted in year 2015 or later.

2. Exclusion Criteria:
    - Studies that are not related to process improvement or cybersecurity.
    - Studies that focus solely on general IT processes without a direct emphasis on cybersecurity.
    - Studies that do not provide substantial information or findings relevant to the research objectives of defining lean ISMS processes or improving cybersecurity in the specified context.
    - Studies that are not available in English.

- Studies that are not accessible freely via chosen databases and instead require subscription.

The eligible studies were categorized into subcategories based on their content. These subcategories included Lean methods, Cybersecurity best practices, cybersecurity assessment, risk management, and cybersecurity in healthcare.

3.2.2 Search strategy

The review material was sourced from two databases: Google Scholar and ProQuest.

The search strategy for the review was developed to ensure relevancy and good coverage on the research subject. To maintain currency and relevance, publications were limited to those released after 2015. Additionally, the strategy required that publications must be in English and readily accessible online, ensuring ease of access for the research. This approach aided in retrieving up-to-date and relevant literature but also streamlined the review process by focusing on publications most likely to align with the research.

The search queries utilized a set of keywords to capture relevant literature to the research. These keywords encompassed various aspects of lean processes, cybersecurity in healthcare, and tools for process improvement, ensuring a comprehensive review of the research domain. Specific keywords used were "lean processes," "healthcare cybersecurity," "cybersecurity assessment," "bottleneck analysis," "Cobit 5," and "NIST CSF," “third-party cybersecurity,” and “software development cybersecurity.”

3.2.3 Selection process

Initial inclusion criteria and search strategy requirements were applied to produce a comprehensive list of relevant studies. This compilation process involved manual screening and evaluation of each potential study utilizing an Excel spreadsheet to organize and manage the records. Subsequently, the titles of the identified records underwent screening to identify and remove any duplicate entries, ensuring the integrity and accuracy of the dataset for further analysis.

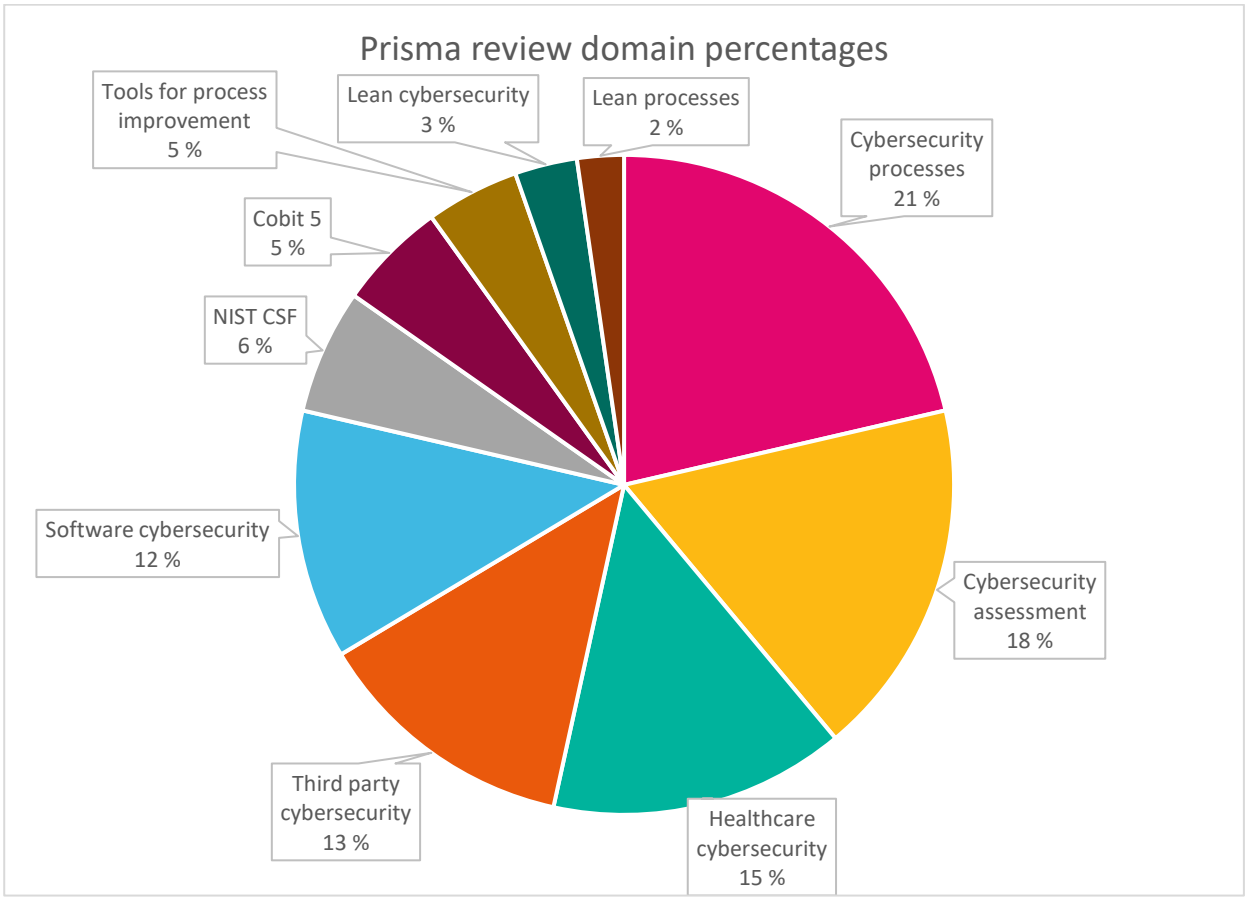

Figure 2. Percentages of included studies categorized to knowledge domains.

Figure 2. demonstrates the distribution of included records in the literature review. The figure describes the various domains of knowledge covered in the review, with research texts related to cybersecurity processes and cybersecurity assessment emerging as the two dominant categories. The distribution depicted in Figure 2. holds some implications for the thesis research as it provides valuable insights into the amount of literature available on the subject matter and describes potential emphasis on some concepts over others.

Study characteristics

This section provides an overview of the results obtained from the search and selection process. Results of this process are depicted in Figure 3. flow diagram.

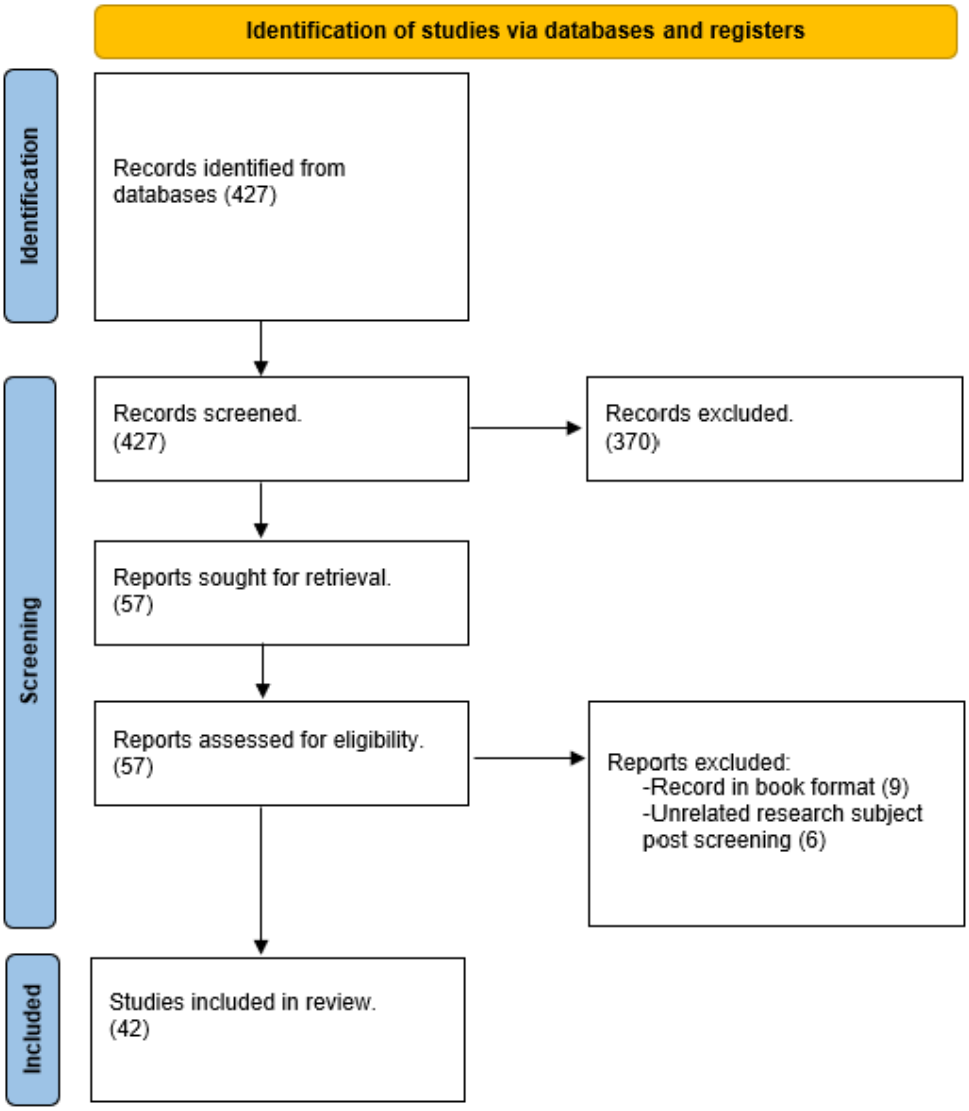

Figure 3. Applied PRISMA 2020 flow diagram.

The initial search yielded a total of 427 records. Following the application of inclusion and exclusion criteria and assessment for eligibility, 42 unique records were identified and included in the review. This screening process ensured that only relevant and high-quality studies were considered for further analysis, improving the credibility and reliability of the literature review.

Initial screening excluded total of 370 records due to extensive number of duplicate records imported from the database searches. Eligibility assessment excluded 9 additional records due to report being a book which was not feasible to study in the timeframe of the thesis work. Also 6 reports were excluded due to appearing to contain unrelated research in context of the thesis work.

3.3 ISMS

An ISMS is the integrated framework within an organization that manages all aspects of information security. It ensures the establishment, implementation, communication, and evaluation of policies, procedures, and objectives to safeguard the organization's information assets (Asosheh et al., 2013).

The establishment, maintenance, and continuous updating of an Information Security Management System (ISMS) demonstrate a systematic approach to identifying, assessing, and managing information security risks. This proactive stance allows organizations to effectively ensure information confidentiality, integrity, and availability, which, in turn, impacts several aspects of their operations. These include ensuring business continuity, minimizing damages and losses, maintaining a competitive edge, enhancing profitability and cash-flow, cultivating a respected organizational image, and facilitating compliance with legal requirements (ENISA, 2022).

IT risk management

Nishani & Pinsker (2020) examined the importance of interrelated activities of IT risk management (ITRM) by researching how one type of ITRM practice can be influenced by the maturity of other organizational ITRM practices. Their model recognized four types of practices: IT governance (ITG), communications, operations, and monitoring. Their research indicates that maturity of a practice helps also in the other areas of ITRM. Conducting mature ITRM can help in other areas of organizational operations, having mature monitoring helps with risk management. Proper communications channels with business functions are emphasized to establish channels to educate and involve other departments in regard of the security of their data.

Security controls and processes

To enhance comprehension of ISMS, it's beneficial to clarify the definitions of controls and processes. A process refers to a series of actions that you take to achieve a result. Control involves monitoring and regulating processes to ensure that they operate effectively and efficiently.

Security controls encompass measures put in place to safeguard critical data and infrastructure within an organization. They serve as safeguards or countermeasures to mitigate security risks, encompassing actions to prevent, detect, counteract, or minimize threats to physical assets, information, computer systems, or other resources (IBM, 2024). On the other hand, processes within ISMS denote the structured workflows or series of interrelated tasks undertaken to manage and maintain the organization's information security.

3.4 Lean

Lean is a methodology that is centered around reduction of waste and doing more with less in organizational operations. Lean operations aim to use fewer resources to generate the same outcome. Operations can be divided into two levels: workplace and strategic. Lean in workplace operations is centered around operational improvements and Lean in strategic operating level is focused on the strategy process and broader organizing philosophy of the organization (Piercy & Rich, 2014).

Alblooshi et al. (2021) describe Lean at an operational point of view as dealing with waste and aiming to speed up and increase process efficiency and base their description on continuous flow of activities, reduction in setup time, high employee engagement levels, continuous improvement, and supplier development. Although their research studied the applications of Lean Six Sigma and not only Lean methodologies. I propose that the challenges to application of the methods apply to Lean as well; lack of management support, lack of awareness, lack of change management and resistance to change, lack of tools and the lack of communication. Ensuring these supportive processes are key part when designing and implementing improved cybersecurity processes. Addressing these challenges is important to gain increased value and competitive edge from organizational processes.

Article written about gaining competitive advantage from cybersecurity lists positive ways that an organization can gain competitive edge through cybersecurity: informing & communicating, simplifying security and making it easy to use, balancing approach to security, understanding technology trends and planning the security architecture, managing a secure supply chain, using incentivizing measurement, embedding security into day-today processes and recognizing and exploiting security opportunities (Investing in cybersecurity, 2021).

Six Sigma and Lean operations appear also in another research by Farahbod et al. (2022). It examined the use of Six Sigma and Lean operations in cybersecurity management. They argued that applying Six Sigma quality management on cybersecurity projects can improve the cybersecurity practices of an organization. They suggested the use of DMAIC (Define, Measure, Analyze, Improve, Control) approach to cybersecurity projects. In their approach they proposed the use of BAR (Business Adjusted Risk) in the measure, analyze and improve stages of DMAIC approach.

This research aims to improve cybersecurity processes on the workplace level using Lean methods from previous studies and their use is described in the following sub-chapters.

3.4.1 Bottleneck analysis

Bottleneck analysis is applied to identify inefficiencies in processes. It is utilized by breaking a process down to individual steps and then measuring the time it takes to complete each step therefore exposing possible bottlenecks (Wolniak et al., 2018). Absence of bottlenecks means that productivity is adequate and aligns with the estimated timeframe.

Bottleneck analysis is divided into four sections: detection, diagnosis, prediction and prescription. Detection is utilized to detect the bottleneck of a process. Detection methods can be analytical, simulation based, or data driven. Diagnosis is utilized to find the root cause of the bottleneck. Prediction methods aim to predict future bottlenecks based on historical data. Prescription is a set of recommendations based on previous methods to improve the process (Mahmoodi et al., 2022).

This research aims to use principles of bottleneck analysis as a tool for process improvement. Processes need to be dissected into smaller tasks to measure the time to complete each of them. Processes measured could be anything from managing cybersecurity to more technical implementations in example the time it takes to deploy antivirus updates on all workstations of the organization.

3.4.2 Respect for people

In Lean thinking, it is emphasized that people who are closest to work are in best position to identify problems and suggest improvements. By actively listening to them, organizations can gain additional information on process problems that could otherwise remain unidentified. This additional information can drive forward the continuous improvement that is in the core of Lean thinking.

Gemba is the Japanese term for “actual place”, Gemba walks refer to a method where managers and executives are encouraged to go to the actual place of work where the value is being created. By observing, listening, asking questions and feedback the organization management can gain information on how to improve processes.

The authors of the journal Strategic Direction (Embracing the unknown by constructing an organizational cybersecurity strategy, 2020**)** propose that organizations need to remain flexible in their cybersecurity strategy and accept unknowns when developing it. They propose ramping up of security processes that are culturally tolerated among employees as an insurance strategy. They also propose that investing in information sharing as an effective way to mitigate cyber threats through preparation activities. In Lean perspective respect for the people acts as an important factor enabling organizations to lessen the effects of unknown by investigating process problems by utilizing Gemba. When the strategy implements feedback from the actual workers, additional security processes can be applied in a way that solves process problems and are inherently build secure in terms of cyber security.

In their article Malatji et al. (2019) propose that when a security solution places too much emphasis on either social or technical aspects it creates a socio-technical gap. This gap can open vulnerabilities that attackers can exploit. Holistically understanding and formalizing the interactions between people and systems without emphasizing one aspect more than the other is called joint optimization that places equal emphasis on social, technical, and environmental dimensions of organisational work practices. To accomplish the joint optimization state of organisational systems security, a balanced set of social and technical controls as influenced by the external environment are required. The social dimension consists of the organizational structure and the people within, to implement balanced controls the respect for the people including Gemba play an important role.

In this thesis respect for the people will be applied through the experiences of the stakeholders of processes to gain better perspective into possible process problems within the organization. In modern information work Gemba can be a challenging concept as the actual work can be distributed widely in physical manner so feedback of the individuals will be the key component utilize respect for the people.

3.4.3 Continuous improvement

Continuous improvement, also known as continual improvement, embodies the perpetual enhancement of products, services, or processes through both incremental and breakthrough advancements. This approach involves endeavors aimed at achieving "incremental" progress over time. Central to the continuous improvement model is the adoption of various methodologies, among which the Plan-Do-Check-Act (PDCA) cycle stands prominent. This four-step quality assurance method encompasses planning, execution, evaluation, and adjustment, serving as a systematic framework for driving ongoing enhancements and ensuring sustained organizational excellence (ASQ, n.d.-a).

In their article, Nicho (2018) proposes and empirically validates an information security governance (ISG) process model utilizing the plan–do–check–act (PDCA) framework. The study emphasizes the dynamic nature of information security, highlighting the need to collaboratively establish a secure environment, thereby promoting a cyclical process of continuous improvement. The research confirms the significance of the PDCA cycle within ISG.

3.4.4 Value stream mapping

Value Stream Mapping is a tool for Lean organizations aiming to improve their processes and efficiency. In their book "Practitioner's guide for statistics and lean six sigma for process improvement" Harry et al. (2010) describe the value stream mapping as one of the most powerful tools in Lean. In their description the production path of value is followed from customer to supplier and visual representation of each process is drawn.

Value Stream Mapping utilizes visualization of the flow of materials, information, and activities from start of the process to the end. With value stream mapping organizations can identify bottlenecks, waste, and opportunities for improvement.

The steps to perform Value Stream Mapping consist of a) identifying the scope of mapping, b) drawing the current value streams, c) assessing current value stream.

Harry et al. (2010) describes in their book that when drawing the current state include the concepts of process time, cycle time, and queuing time. In information work settings, tasks frequently involve non-routine activities characterized by variability and unpredictability. Unlike traditional manufacturing processes where tasks are standardized and repetitive, knowledge work often entails unique challenges and requires adaptive strategies. Consequently, traditional metrics such as process time may lack relevance.

Additional improvement steps can be taken to d) create “future state” value stream map, e) developing an implementation plan, e) implementation according to plan, f) review and iteration of the implementation. Harry et al. (2010) poses a question that guides the design of the future state value map: "What can we do to improve what we have?" The designer of the future state value map is tasked with conceptualizing a vision that overcomes the limitations and challenges of the current state.

Value stream identification and scope

To identify the scope for the value stream mapping the product or service needs to be selected first. Then the start and end points of the process need to be defined. To ensure clarity of the VSM a specific aspect of the process should be focused upon. In example in case of product development the VSM could focus on the value stream of assembly line process.

Key stakeholders need to be engaged including personnel directly involved in the process to gather necessary data on the process. Tasks involved in the process need to be organized so that the value map depicts the current state accurately. Each task needs to be assessed for its value adding potential to identify points that increase value and areas of waste. Tasks that do not add value can be eliminated or optimized.

Value stream improvements

Improving the value stream starts with envisioning the future state of the value stream where constraints are eliminated via lean principles and best practices. Harry et al. (2010) describes them as value-added and non-value added activities that inhabit the process stream. Bottlenecks need to be eliminated and opportunities of improvement utilized.

After future state value stream is created an implementation plan must be developed. The goals and improvement objectives need to be derived from the plan and relevant stakeholders need to be included in the planning process. Implementation of the plan can be executed utilizing Lean methodologies such as Kanban to execute changes systematically and enabling easier progress monitoring. Challenges faced on process changes can then be assessed and mitigated on per task basis. The outcomes of implemented process changes needs to be evaluated and their improvements in efficiency, quality, and customer satisfaction need to be measured. Lean philosophy emphasizes continuous improvement so reviewal of processes should be done regularly.

In their research Alvarenga & Tanev (2017) suggest that there is a gap on research how to address cybersecurity concerns in a way that brings value to all relevant stakeholders. They suggest that cybersecurity can be used as a value proposition to the stakeholders. In the perspective of this thesis research value will be treated from cybersecurity perspective where the end value is a product where the confidentiality, integrity, and availability have been ensured. Thus, value stream mapping, especially the future state should be envisioned in a way that focuses on those aspects as the end value.

3.4.5 IT security and product development in agile organizations

According to Poth, Kottke, Middelhauve, Mahr, and Riel (2021) organizations that maintain agile development teams can integrate IT security and data privacy regulations into the agile workflow. This is implemented with the use of shared responsibility model to regulations and by applying Level of Done -layers (LoD-layers). Shared responsibility and accountability of compliance to regulations is achieved with shifting from classical centralized governance to autonomous development teams: LoD-layer implementation is achieved by layering requirements of different regulations or standards and filtering to where they should apply. Example of LOD-layers

implementation would be Chief Information Security Officer (CISO) being accountable for ISO 27000 regulations, but Local Information Security Officer (LISO) would then enforce these regulations on their specific business domain. The enforcement would include the selection and refinement of the relevant aspects of the regulations (Poth et al., 2021). In agile development team the LISO would usually be the product owner.

3.5 Threats to healthcare sector

Healthcare information technology (HIT) offers many benefits for healthcare organizations in improving the care of their patients. However, this technology exposes them to new vulnerabilities arising from increased connectivity of devices and digitalization of information. In their research Bhuyan et al. (2020) make an argument that cyber breaches result in a greater average cost for healthcare organizations which already are constrained with high expenditure and low-profit margins. Additionally, high volume of sensitive data containing protected health information of patients make healthcare organizations a lucrative target for cybercriminals.

In context of this thesis research, it is imperative to study the different methods of attacks against healthcare organizations and research how information security processes could be improved to better protect against them.

3.5.1 Challenges and Threats in Healthcare Cybersecurity

Cybersecurity breaches in healthcare can compromise the core principles of information security: confidentiality, integrity, and availability. The healthcare sector is particularly vulnerable to cyberattacks due to weaknesses in its systems, including hardware, software, networks, and human factors. In their research Aljuraid and Justinia (2022) examined existing literature to investigate cybersecurity threats to cybersecurity. After their initial literature review the authors selected 62 different articles according to their relevance on the topic. The articles were then analyzed and the threats from the articles were composed on the following table.

Table 1. Famous threats in healthcare organisations.

Type of Threat	The Threat	Threat's Level	The Potential Motives
Not announced	Malware: Contagious	Medium	Disrupt the system, preparing to break through the system.
Not announced	Malware: Masked	Medium	Disrupt the system, stealing sensitive information (e.g., login credentials).
Not announced	Malware: Others (e.g., Ransomware)	High	Obtaining money by demanding ransom, data breach is unlikely
Not announced	Denial of service attacks	High	Disrupt the system, preparing to break through the system, and demanding payment, data breach is unlikely
Cybersquatting	Phishing	Medium	Lead to data breach, obtaining sensitive information to sell on the dark web. May lead to other types of attack, such as ransomware and other misuses of data for financial gain
Cybersquatting	Masquerade attacks	High	Obtain sensitive information and delete or modify health related information that could lead to harming the patients
Cybersquatting	Data injection attack	High	Incorrect diagnosis, illegal insurance claim, and mission critical factors
Technological threats	Hardware/softw are errors or	Medium	Usually unintentional, though could lead to

	failures		unreliable services
Technological threats	Obsolete technology/out of date HIS	Medium	Usually unintentional, often resulting in untrustworthy and unreliable systems
Technological threats	Critical infrastructure or power failure	High	Usually unintentional, but severe consequences could occur, such as data loss
Insider threats	Human usability error	Low	Usually from unintended negligence of the employees, hence, represents a serious risk to confidentiality and privacy
Insider threats	Management weakness	Medium	Often unintentional due to staff and budget limitations, or overall lack of experience

Note, Reproduced from Challenges and Threats in Healthcare Cybersecurity (p 364) by R. Aljuraid and T. Justinia, 2022

In their research Loi et al. (2019) studied the value tensions between core values of health systems and cybersecurity. They mapped relevant objectives of ICT, quality and efficiency, safety, privacy, and usability to four principles of medical ethics, beneficence, non-maleficence, autonomy, and justice. This allowed them to map trade-offs between goals of cybersecurity and the four principles. They suggested that prioritizing some values will come at the expense of others e.g., prioritizing beneficence and autonomy will come at the sacrifice of justice. In example a process that maximizes amount of data produced and analyzed could cause loss of privacy of patients. These findings should be considered when designing a lean process for a healthcare organization. The process cannot maximize usability and efficiency at the cost of core values. This requires thorough planning and assessment to find areas of improvement that will not cause harm to the patients or other stakeholders.

3.5.2 Supply chain risk

In their study, Ghadge et al. (2020) describe the concept of the cyber supply chain as a network of IT infrastructure and technologies facilitating data sharing in virtual networks, introducing risks not related to physical products or specific physical locales. The research emphasizes the pivotal role of human and behavioral factors in cyber security risk, identifying a tendency to prioritize technical risks over behavioral ones. It advocates for heightened risk awareness, standardized policies, collaborative strategies, and empirical models to foster cyber resilience within the supply chain ecosystem. The result aligns with the conclusion of Koskinen (2023) research that cybersecurity is realized when organizations make informed decisions based on well-prepared, understandable, and presented information.

In healthcare cybersecurity context, third-party involvement may pose significant challenges. Healthcare organizations rely on third-party vendors for services like cloud storage and medical devices, but these partnerships also introduce vulnerabilities. Third-party vendors may not have the same security standards, creating potential vulnerabilities. Breaches in vendor systems can have extensive effects, compromising patient data confidentiality, integrity, and availability.

3.5.3 Protecting against cyberattacks

In their research Bhuyan et al. (2020) list approaches to gain resilience against these attacks. Organizations should take a comprehensive approach to their management of IT objects rather than ad hoc response of threats case by case. The comprehensive approach includes governance over each process that ensures planning, training, financing, and other factors are adequate to achieve improved resilience. The authors also mention risk management as another approach to improve resilience. This approach involves identifying potential risks and once each risk is identified, the vulnerabilities to specific assets are determined. The also suggest incorporating cybersecurity into strategic planning and budgeting processes.

Bhuyan et al. (2020) list six different types of cyberattacks that can harm any organization:

-Denial-of-Services (DoS) attacks that aim to disrupt services and prevent users from accessing them by flooding the network with traffic.

-Privilege Escalation attack that aims to gain a higher level of access to a system than was originally intented.
-Man in the Middle (MITM) attack which eavesdrop communications between devices e.g., servers.
-Cryptographic attacks which are intended to decrypt encrypted information
-Structured Query Language (SQL) injection exploits which aim to make vulnerable SQL services divulge otherwise protected information.
-Phishing attacks that aim to use social engineering to make individuals or organizations perform harmful actions against their own information security.
-Malicious Software such as viruses, trojans, spyware and ransomware which can harm the confidentiality, integrity and availability of services of infected systems.

3.6 Results of literature review

In this section, the outcome of the literature review is discussed, summarizing the findings, insights, and conclusions derived from the analysis of relevant research. During the development phase of the thesis work it was noted that the focus of the research was not on all the knowledge domains of the literature review. Consequently, chapter considering cybersecurity frameworks has been excluded.

The literature review consists of an exploration of Information Security Management Systems (ISMS), emphasizing the interconnected nature of IT risk management activities and noting how the maturity level of one aspect of IT risk management can significantly impact other organizational practices within the framework. Furthermore, the review contains the application of lean methodologies to streamline processes by minimizing waste and optimizing efficiency. Additionally, the identification and mapping of threats within the healthcare sector shed light on the need for cybersecurity measures. Lastly, the relevance of third-party involvement in the supply chain is acknowledged, highlighting its significance in bolstering cybersecurity resilience.

In conclusion the author observed no evident bias, and the research included a comprehensive selection of records from various domains within the eligible literature. The sources were retrieved from reputable research databases, ensuring a high level of certainty and reliability of the evidence obtained.

After the literature review the thesis work has been appended by 10 sources of information containing information about the case organization, definitions of concepts, and regulatory parties in Finland. The sources were implemented to broaden the knowledge base of the thesis work and to provide necessary information not found in the research literature.

4 Development process

In this chapter the development of processes is described. Data from gathering phase is analyzed and cross referenced. Lean methods are applied to selected controls and processes behind them. The chapter consists of gathering relevant data for development, analyzing development data, confirming the results of analysis, and selecting most valuable processes.

4.1 Data gathering

This chapter describes the data gathered in addition to the literature review. This includes summary charts of incidents and cyber threats facing Fimlab and Pirha as an organsation, review of organisational controls related to said threats, and how data was gathered from workshops with stakeholders.

4.1.1 SOC reports

Reports from security operations center service (later referred as SOC) provided for Pirha and Fimlab were gathered and incidents from them were summarized by category. Charts were formed from the data to represent the categories and frequency of incident type. Percentage of incidents are shown in two different charts, one displaying the incidents categorized in a freeform manner using self-described categories by author (Figure 4.) and the other chart (Figure 5.) displays the same incidents categorized using Enisa taxonomy. Taxonomies are later explained in chapter 4.1.3.

Reports range from March 2022 to November 2023 and the charts formed are meant to provide a practical view on the everyday threats to healthcare organization information security. During the timeframe 26 different kinds of incidents were included in the monthly reports of the SOC.

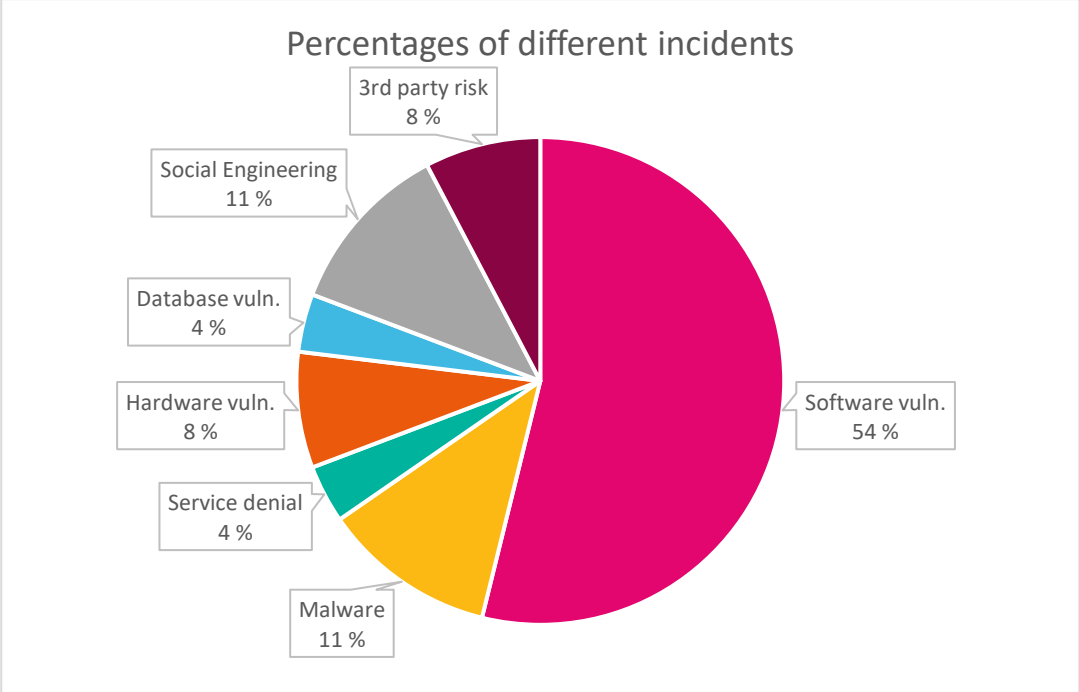

Figure 4. Freeform categories and percentage of incidents categorized.

It is worth noting that Figure 4. contains more categories that Figure 5. and thus provides a more detailed description on the nature of the incidents. Figure 5. contains more generalized and clearer depiction on the nature of the incidents and it uses the Enisa taxonomy.

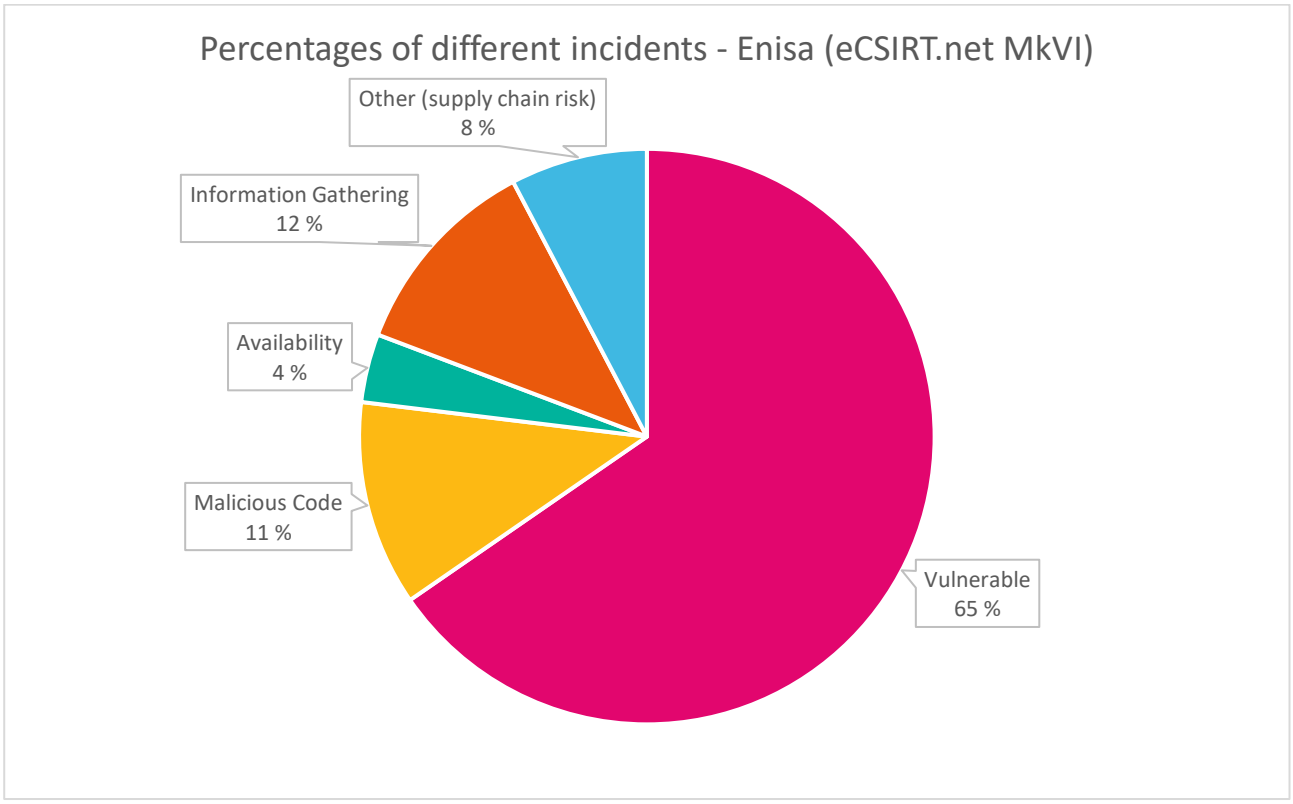

Figure 5. Percentage of incidents represented with Enisa taxonomy.

Remediations for the incidents are depicted in figure 6. It contains total of 30 remediation efforts. The remediation categories are freeform categories using self-described taxonomy by the author. It is worth noting that the amount of remediations is greater than the incidents due to some incidents requiring multiple types of remediations.

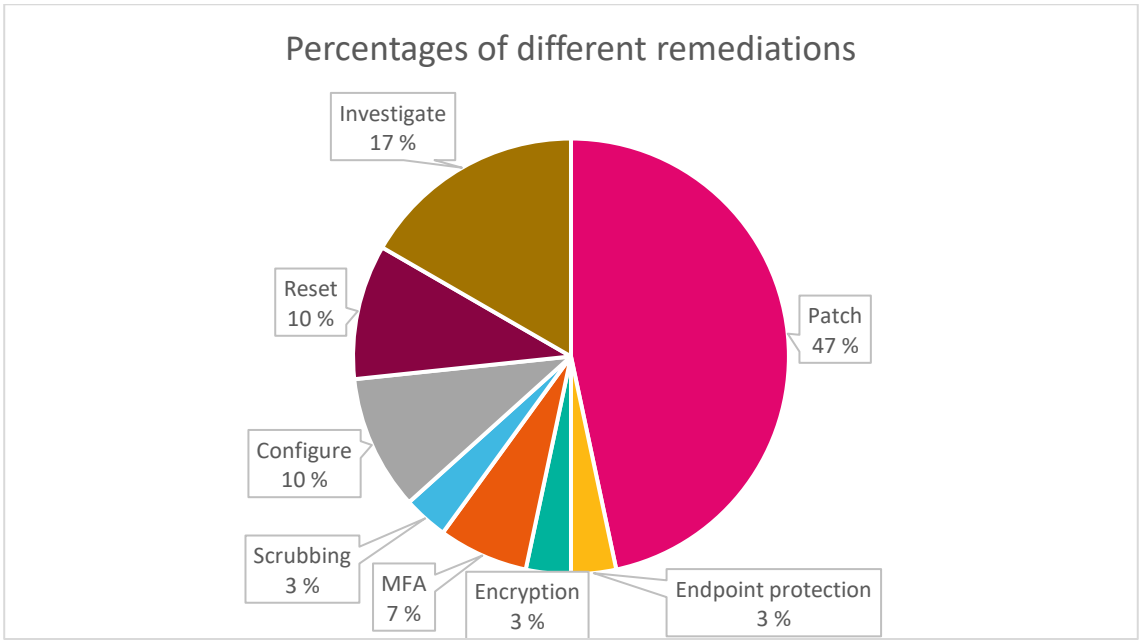

Figure 6. Percentages of different kinds of mitigations

4.1.2 Major incidents

Major incidents in the organization are incidents that are remediated following Pirha's Major Incident Management (later referred as MIM) protocol. These incidents are information security incidents in the sense that they greatly affect the availability of services and data and can pose even life-threatening consequences to patient care as described in the background chapter of this thesis.

Case organizations major incident log was reviewed from the same time range as the SOC reports and incidents were summarized and categorized using authors own taxonomy. The log contained 71 different major incidents and same amount of remediation efforts. Figure 7. describes the major incident categories in authors own taxonomy.

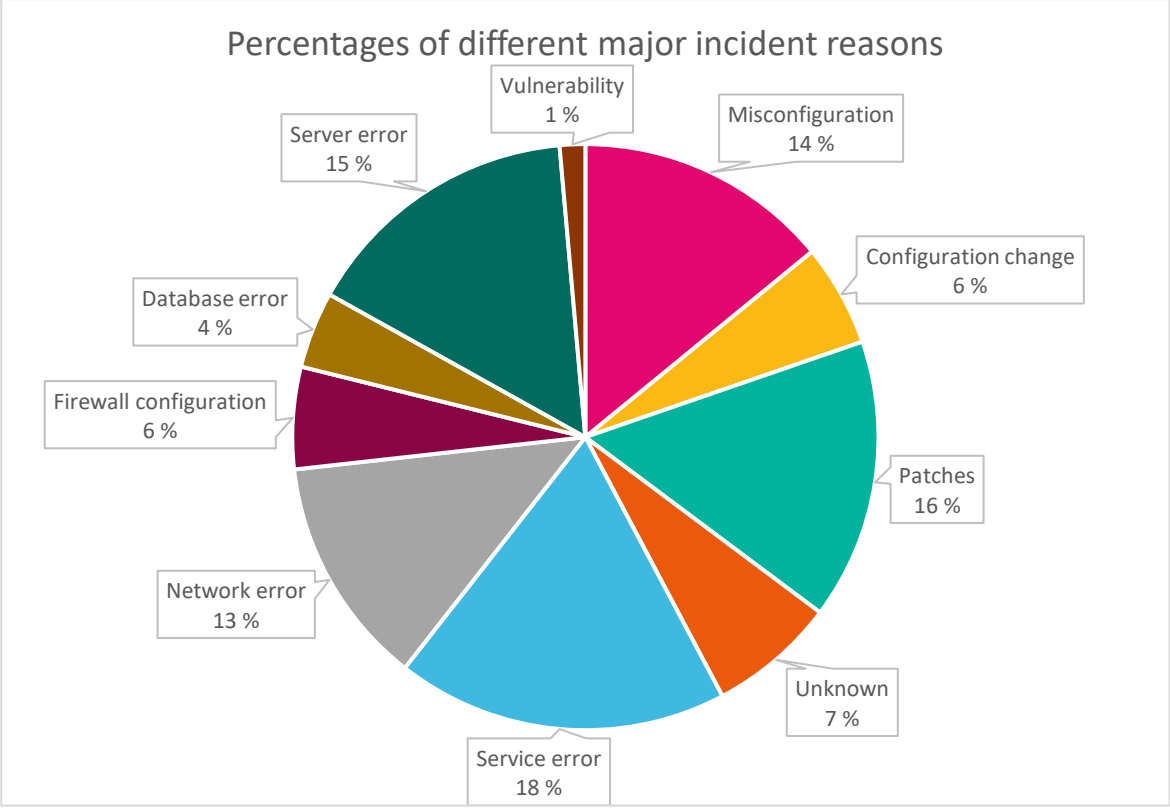

Figure 7. Percentages of major incidents reasons

In Figure 8. the efforts made in the MIM process to remediate the incidents are presented. Remediations are categorized using authors own taxonomy.

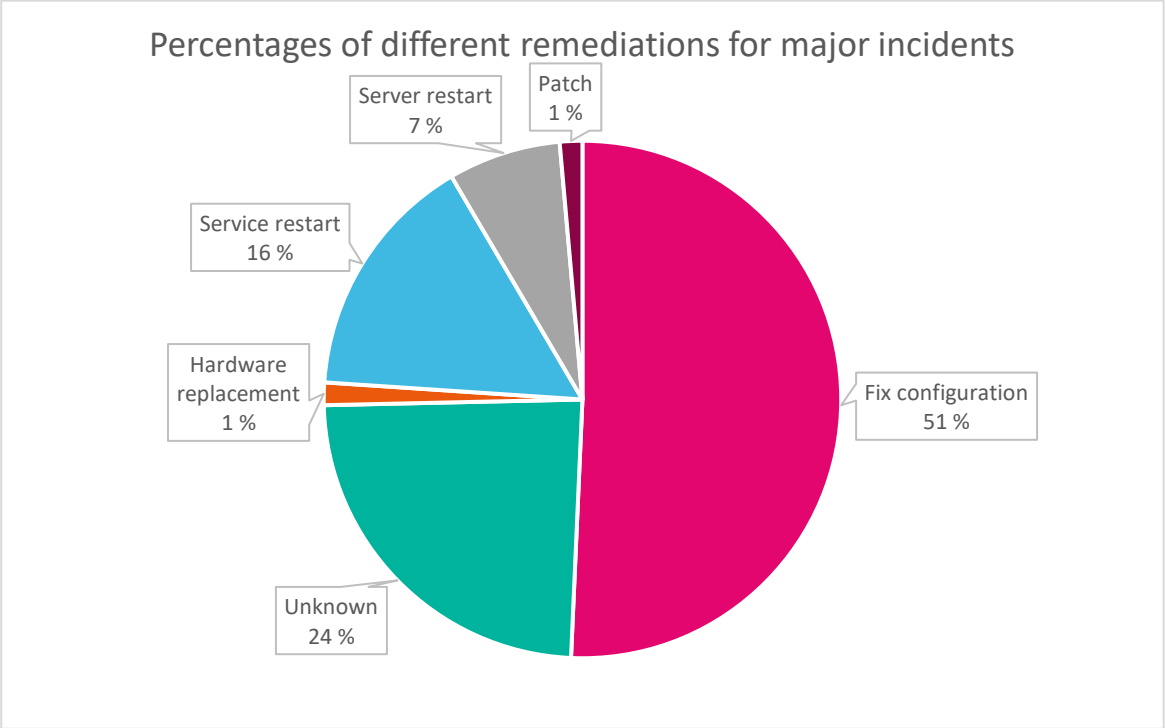

Figure 8. Percentages of major incident remediations

4.1.3 Taxonomies

The incidents and remediation reviewed from SOC reports and incidents logs were categorized to better identify the connected controls and processes related to the categories later in the process design phase of the thesis.

Two different taxonomies were used to categorize the events. First table in this chapter contains Enisa reference taxonomy (Enisa, 2018) and the second contains authors own description of incidents and remediations based on report and log descriptions. The two tables contain the category names, whether the category uses self-described or Enisa taxonomy, short description of the category name and the figure number in which figure the category is used.

In self-described categories the descriptions are written in context of the charts instead of general description of the term meaning. In the Enisa taxonomy table (Table 2.) the descriptions include only the SOC and MIM specific descriptions. Also, in addition the category “Other” was appended with additional information “supply chain risk” to emphasize the actual incidents since no official category was not available through Enisa taxonomy.

It is to be noted that major incidents of the log reviewal were not separately mapped to Enisa terms at all since in Enisa reference taxonomy the major incidents of Figure 7. are all classified as availability incidents. This will be noted on the data gathering and validation workshops when chart data is presented to the relevant stakeholders.

Table 2. Enisa reference taxonomy and descriptions.

Name	Author	Description	Figure number
Vulnerable	Enisa	Open resolvers, world readable printers, vulnerability apparent from scans, virus signatures not up to date	4
Malicious code	Enisa	Software that is intentionally included or inserted in a system for a harmful purpose.	4
Availability	Enisa	By this kind of an attack a system is bombarded with so many packets that the operations are delayed or the system crashes. DoS examples are ICMP and SYN floods, Teardrop attacks and mail-bombing. DDoS often is based on DoS attacks originating from botnets, but also other scenarios exist like DNS Amplification attacks. Also local actions such as disruption of power supply, spontaneous failures or human error, without malice or gross	4

		neglect being involved.	
Information Gathering	Enisa	Gathering information from a human being in a non-technical way (e.g. lies, tricks, bribes, or threats).	4
Other (supply chain risk)	Enisa, self-described	If the number of incidents in this category increases, it is an indicator that the classification scheme must be revised. Supply chain risk a→	4

Note, Reproduced from Reference Incident Classification Taxonomy (p 9-10) by European Union Agency for Network and Information Security, 2018

Table 3. Self-described categories of incidents and remediations

Name	Author	Description	Figure number
Software vuln.	Self-described	Software vulnerabilities detected in IT systems used by the organization.	3
Malware	Self-described	Malware detected by SOC.	3
Service denial	Self-described	Cyberattacks detected in SOC that result in denial of service such as DDOS attack.	3
Hardware vuln.	Self-described	Incidents detected by SOC that relate to vulnerabilities in the hardware of mobile	3

		devices, desktops, laptops, servers and medical devices.	
Database vuln.	Self-described	Vulnerabilities detected by SOC in databases, such as SQL injection.	3
Social engineering	Self-described	Social engineering incidents detected by SOC, such as phishing and pretexting.	3
3rd party risk	Self-described	Incidents reported by SOC that are purely caused by 3rd party non malicious actions.	3
Endpoint protection	Self-described	Remediation of information security incident through automated endpoint protection actions.	5
Encryption	Self-described	Encryption of unencrypted traffic as a remediation.	5
MFA	Self-described	Remediation of information security incident through multi-factor authentication protocol.	5
Scrubbing	Self-described	Use of scrubbing services to mitigate denial of service attack.	5
Configure	Self-described	Configuration of service to remediate information security incident.	5
Reset	Self-described	Reset of a user configuration to remediate	5

		information security incident.	
Investigate	Self-described	Investigation to servers and services to identify vulnerable assets.	5
Misconfiguration	Self-described	Non malicious configuration of service that led to loss of service availability.	6
Configuration change	Self-described	Non malicious configuration change on a service that led to loss of availability of service.	6
Unknown	Self-described	Can appear as incident cause or remediation. Unknown reason for loss of availability of service or unknown remediation to the root cause. Mainly caused by external service providers not providing sufficient data or lacking documentation of major incident process.	6,7
Service error	Self-described	Error in running services of a server leading to loss of availability or corruption of data.	6
Network error	Self-described	Error in network operations leading to loss of availability of services.	6
Firewall configuration	Self-described	Firewall specific configurations that led to	6

		loss of availability of services.	
Database error	Self-described	Database specific error leading to loss of availability of service or integrity of data.	6
Server error	Self-described	Malfunction in server leading to loss of availability of services.	6
Vulnerability	Self-described	Vulnerability in servers or services that caused loss of availability.	6
Fix configuration	Self-described	Change in configuration of server or service to remediate incident.	7
Hardware replacement	Self-described	Remediation to major incident caused by hardware malfunction.	7
Service restart	Self-described	Restart of service to restore availability of service.	7
Server restart	Self-described	Restart of server to restore availability of service.	7
Patches, Patch	Self-described	Updating and patching servers or services to remediate vulnerabilities. Also appears as an incident category due to loss of availability from unexpected repercussions of the update or patch.	5, 7

4.1.4 Process workshop

After pre-analysis of incident and remediation data a workshop was organized to validate the results from data gathered and to gather additional information from the relevant stakeholders regarding related cybersecurity processes. Tentatively gathered organizational documentation on processes related to patching of IT systems and the introduction of new IT systems was assembled to be presented to stakeholders. The stakeholders were also inquired about additional information regarding documentation on related processes. Additional information on challenges and problems regarding patching operations and change management was also requested.

The presentation material used in the workshop is presented in chapter “Data analysis” in the subchapters “Pre analysis of incident and remediation data” and “Organizational controls”.

4.2 Data analysis

4.2.1 Pre-analysis of incident and remediation data

During the review of major incident and SOC report data an observation was made that in SOC reports patching systems was a frequent remediation. On the other hand, issues related to patching were quite frequently seen as the root cause of issues in major incident data. This was noted in the upcoming workshop material for further discussion on relation of patching and availability issues.

Valuation of processes related to mitigation of frequent issues versus otherwise critical issues, in example patching vulnerabilities versus recovering from cyber breach, is an issue that will be noted in this thesis work when choosing what cybersecurity processes to develop. In Lean terms processes are measured by the value that they generate. Are processes that control the remediation of frequent incidents more valuable to organization than those that control remediation of infrequent but critical incidents?

Workshop

Workshop was organized with stakeholders that hold responsibility in areas of network, server, and application development management. The results of incident analysis on SOC-reports and incident calendar were reviewed and generally agreed on. The stakeholders were presented the following questions:
-What is the correct balance between the values of cybersecurity operations and healthcare operations?
-Were the results of the incident review consistent?
-What is the role of external organizations in Fimlabs incident management?

In addition, there were additional questions that were left unanswered due to limited time of the workshop:
-What process is more valuable, one that remediates a critical problem or one that remediates a common problem?
-What documentation is available on cybersecurity processes?

Four people from the organizations IT-management attended the workshop including me, they will be referred as participant A, B, and C. They are responsible of network operations, software architecture and server management. Also, later in this chapter several service providers of the organization will be referred as service providers X, Y, and Z. They provide the organization with service desk, server administration and network services.

At the beginning of the workshop the research questions of this Thesis were represented to the participants and the research approach to information security that this work takes was explained. This consisted of defining cybersecurity with the CIA triad: confidentiality, integrity, and availability. Additionally, a model on the approach to processes and controls was explained.

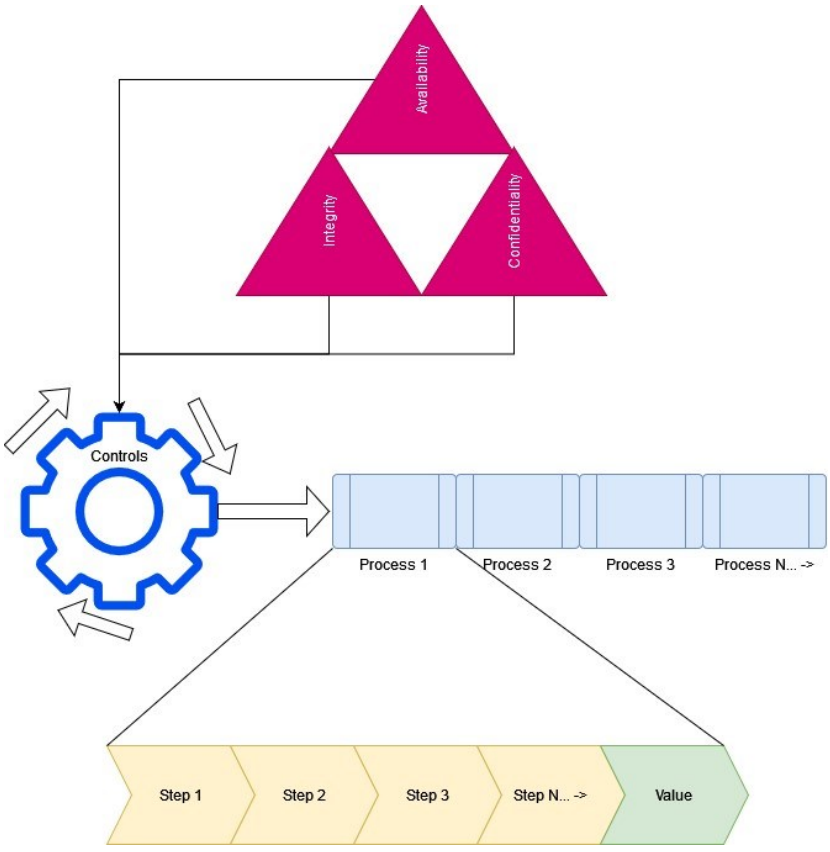

Figure 9. Control, process, and phase model relating to CIA triad.

In the next stage of the workshop the data gathered from SOC reports and major incident log was represented. The same data is represented in Figures 4, 5, 6, 7, and 8. Lastly a hypothesis and a synopsis of the data was represented. The hypothesis was that system development and new vulnerabilities lead to patching which in return causes availability problems quite often. Remediations

to availability problems largely consist of configuration fixes and in some cases the fix is undocumented. This could be due to external party performing the fix or other difficulty in information flow towards the internal organization.

Workshop discussions

After the presentation discussion was held on about the relation of SOC incident reports and major incident logs. Even though SOC incidents were sourced from reports that affect the whole of Pirha, it was agreed that it represents sufficiently the cybersecurity challenges that Fimlab as a singular organization also faces. Patch management was seen as working generally well when applied on internally developed systems, but externally administered systems were seen more vulnerable to misconfigurations and availability issues after patching. The documentation of incident root causes and remediations to those issues were also lacking mostly on the externally administered systems.

This is because of our contractual relations . . . I have understood that with every major incident service our provider X performs problem management, which includes root cause analysis. We have not had that contract with them. The contract has been between Pirha and the service provider. In our current state we do not have that. For every major incident a root cause analysis should be performed so we know why it happened and what has been done to repair it. It is missing from our process. Root cause analyses could have beneficial effect in the future . . . Although we do seek for the root cause. I cannot remember a major incident, where to root cause had not eventually been found out. It just might not get written down . . . In process point of view, it should be focused on that the root cause is easier to write down and when the mitigation has been done. We should strive for light and fast processes, but it [the additional documentation] should be written down . . . we should be able to see [from earlier documentation] if similar incident has been mitigated and how it has been done." (Participant C, workshop discussion translation, December 18, 2023)

It was noted that many availability issues could be quickly remediated through automation scripts, but again it was seen hard or impossible to apply such mitigations to systems that were not directly administered by Fimlabs internal development teams due to restrictions on service policies. Patch management was seen difficult also due to vulnerabilities occurring on multiple levels of system architecture. Vulnerabilities were seen as occurring on three levels: hardware, operating system, and software level. Hardware and operating system level vulnerabilities were seen as easier to investigate and remediate, but software level vulnerabilities were seen challenging to control due to the large amount of sometimes unknown external components used in code.

"If you think about Log4j vulnerability it is quite hard to patch all systems. It can be part of our software through many routes. Consider a largely used code library which includes a vulnerable component . . . Service provider Y built us a script which iterated through the whole filesystem [of the servers] to see which one has log4j-component. Of course, it does not give us a final answer [were all affected servers located] . . . scanning for vulnerabilities on systems can be sometimes challenging and time consuming . . . OS level patch management is easier than trying to patch the vulnerabilities of the software running on top of the operating system. Dynatrace is used on some of the systems for this [software vulnerability scanning] . . . only the most critical applications are scanned by it. And if we find a vulnerability with it . . . patching it usually affects the operations of the application . . . and if it is not our internally developed software, but acquired from an external vendor . . . then it might be really hard to get patches for it . . . mitigating vulnerabilities from software like that, I think it must be done by deploying zero-trust architectures and defining strict network rules . . . for our internal development we also have sonar cube to analyze for vulnerable libraries, but that's internal development only . . . for external I do not think we have posed any requirements [about vulnerable software components] to them." (Participant C, workshop discussion translation, December 18, 2023)

” If we posed such requirements, it is unclear what the response might be . . . in some cases it seems that they see themselves more as a device provider than software provider . . . where in fact they are software providers (Participant B, workshop discussion translation, December 18, 2023)”

” We must recognize the different levels on patch management [hardware, OS, and software] and define different types of processes for them (Participant C, workshop discussion translation, December 18, 2023)”

Again, the greatest challenges were observed on systems whose development was on the responsibility of external development teams. Also, acquirement of secure systems was seen challenging from time to time due to unavailability of such systems from vendors. The security requirements for IT-system acquisition were also seen as in need of refinement.

It was observed that in some cases it was unclear for those responsible of IT-acquisitions on how to utilize the requirements set by IT-administration and since there is two sets of different requirements it was unclear which one of them to choose.

” At this moment when we ask for price references and do competitive bidding [for software and system acquisitions] we do have the basic documentation for information security requirements. I think we should bring stricter requirements to the biddings. In that way we can demand more specific information security aspects from the software and take the responsibility to the vendor. We have two types of requirements depending on if the software will be handling personal data.” (Participant C, workshop discussion translation, December 18, 2023)

” [when the vendor can’t meet all the information security requirements] requirements must be adapted in some cases, but they should be in-line no matter what competitive bidding it is . . . in

the past there are few cases that systems were acquired without consulting the security requirements first." (Participant A, workshop discussion translation, December 18, 2023)

"One thing is the security assessment of new systems and applications . . . the ones we do today might not be so uniform . . . we should readjust the process on biddings and how we evaluate if something is in-line with our security requirements . . . also the security assessment should be more agile but also more accurate." (Participant C, workshop discussion translation, December 18, 2023)

Other problems regarding the availability of systems were observed on the network operations.

"Majority of our remote office networks are from service provider Z; they are responsible for configuration changes and updates on that part . . . there are some cases [that there has been a disruption in availability after update] . . . but we rarely get to know the root cause through service provider A . . . there has been quite a lot of configuration mistakes as well . . . also in some remote offices better service level agreements are unavailable . . . the network monitoring of service provider A does not always work, sometimes we've had to notify them that our remote office has connection problems before they've even started to react" (Participant C, workshop discussion translation, December 18, 2023)

At the end there was discussion on how the organization would develop its own change management processes to replace the ones that were implemented through Pirha. It was seen that information security should be built into the acquisition process. In that way when a new system is acquired and brought to the change management process the security issues would be more manageable and better acknowledged.

Workshop discussion implications

The results of the workshop implied that processes related to IT system management of external systems should be reviewed for bottlenecks that impact negatively on the value gain from the processes. In the context of this thesis, processes related to the acquisition of external IT-assets, ranging from acquisition to development and maintenance, incident troubleshooting and recovery, and finally decommissioning of the asset. Related processes will be analyzed with Lean methods such as bottleneck analysis, value stream mapping and waste reduction and work standardization to better optimize the use of organizational resources and gain increased value in information security perspective.

In Figure 10. the main steps in IT-asset lifecycle related to this thesis are represented. The means to optimize the processes related to steps in Figure 10. could in example be:

-Revising security requirements for acquisitions.
-Enforce the use of security requirements.
-Establish change management.
-Make acquisitions part of the change management process.
-Perform cybersecurity risk assessment and data protection impact assessment as part of the change management.
-Develop a standardized governance framework for maintenance of outsourced IT assets, including centralized communication channels.
-Regularly review assets that they adhere to agreed-upon security requirements with service providers.
-Establish standardized process for root cause analysis and incident reporting.
-Regularly review and refine related cybersecurity processes as part of the continuous improvement agenda.

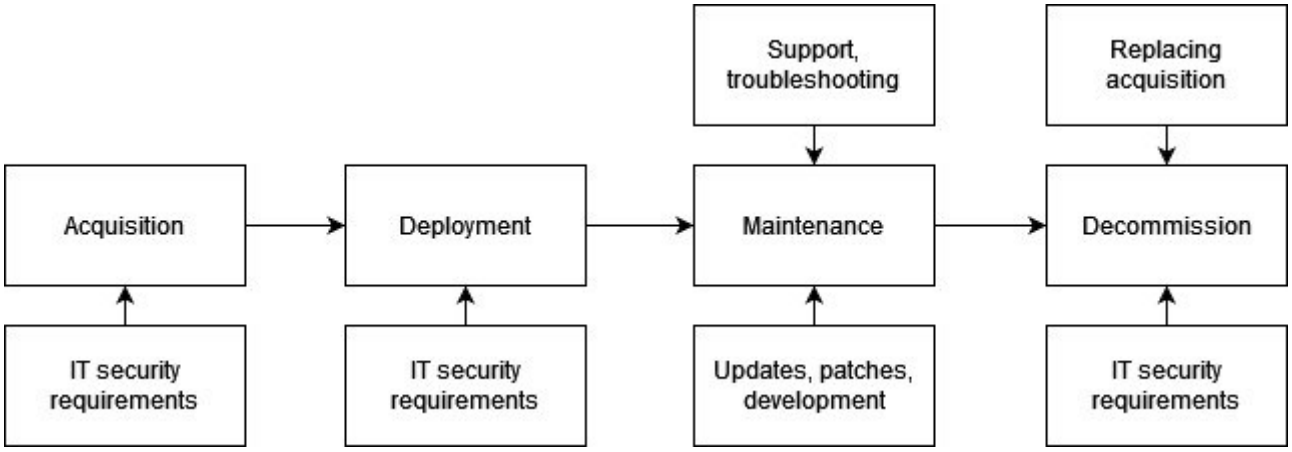

Figure 10. Simplified IT-asset lifecycle

Since the workshop discussions and implications are only personal pickings from the discussion data perceived by the author to be important the conclusions need to be tested. Before applying any of the proposed optimization steps further analysis needs to be applied to the data acquired from major incident calendar, SOC reports and workshop discussion data. This analysis will guide what optimization steps can be valued over others and will provide necessary detail to possible problem points.

4.2.2 Data mapping and conversion

A table was constructed containing the data from Table 1 (Famous threats in healthcare organizations), SOC reports and major incident calendar. The table is divided into six sections each containing calculated multiplier or score. Each section and the justification behind the scoring system will be discussed in greater detail in the following subchapters. A row from the table 1 constructed from original study of Aljuraid and Justinia (2022) was intentionally left out containing the category “Management weakness” with motive description “Often unintentional due to staff and budget limitations, or overall lack of experience”. This was seen as hard or impossible to map to either SOC or MIM processes and was seen to provide no value for following analysis of the processes behind SOC and MIM controls. The constructed data is presented in Table 4.

Threat category (TC)

Threat category section consists of three columns: Threat category, Threat's level, and Threat points.

Threat category is reproduced from the Table 1. It contains category name with a possible subcategory i.e. category "Malware", subcategory "Contagious".

The next column is Threat's Level. This is also reproduced from Table 1. and contains the perceived threat level of the original study of Aljuraid and Justinia (2022). Next column is Threat points which is a numerical conversion of the Threat's level column.

The justification for the numerical conversion is to provide qualitative data for total point calculations later in this study. The conversion scale is from 1-3 responding to their respective nominal categories: Low, Medium, and High.

Matching SOC Incident category to threat - Enisa (SIG)

This section contains the columns: Matching SOC Incident category to threat - Enisa (SIG), Percentage of total incidents in category, and SOC Multiplier.

Matching SOC Incident category to threat - Enisa (SIG) -column represents data from SOC reports where the SOC incident had similar categorization to the threat category from Table 1. The column uses the Enisa taxonomy categories instead of the freeform categories depicted in Figure 5. to provide lesser number of categories and more generalized data for improved comparison to major incident categories.

Percentage of total incidents in category -column provides a percentage depicting how often the SIC appeared in gathered SOC-reports. SOC-Multiplier -column provides a multiplier that is calculated from the SIC-value with formula: 1 + SIC percentage. In example TC "Malware: Contagious"

had matching SIC named “Malicious code” with appearance percentage of 11%. Utilizing the formula, the calculated multiplier is: 1 + 0,11 = 1,11. The multiplier describes how often a SIC is related to SOC operations.

The justification for the multiplier is to later utilize the multiplier with the SOC effort multiplier to calculate how much a threat category occupies the resources of SOC operations.

Related SOC incident remediation (SIR)

This section contains the columns: Related SOC incident remediation (SIR), Percentage of total remediations in categories, and SOC effort multiplier.

Related SOC incident remediation (SIR) -column represents the remediation categories from SOC operations. In example of the SIC “Malicious code” the SIR-value represents all the remediation categories related to remediating malicious code incidents: Patch, Investigate, and Endpoint protection.

Percentage of total remediations in categories -column describes the total appearance amount of remediation categories in gathered SOC -reports. In example of SIC “Malicious code” the related remediations: Patch, Investigate, or Endpoint protection appeared in total of 67% of the total incidents.

SOC effort multiplier -column provides a multiplier that is calculated from the SIR-value with formula: 1 + SIR percentage. In example TC “Malware: Contagious” had matching SIR remediations with appearance percentage of 67%. Utilizing the formula, the calculated multiplier is: 1 + 0,67 = 1,67. This multiplier is used with SOC multiplier to later calculate the total points of a TC. SOC multiplier and SOC effort multiplier score multiplied together describe in quantitative terms how much a SIC utilizes SOC resources.

Matching major incident category to threat (MIG)

This section contains the columns: Matching major incident category to threat (MIC), Percentage of total incidents in categories, and Major incident multiplier.

Matching major incident category to threat (MIC) -column represents the data from major incident reports where the root cause of incident (major incident category) had a matching TC. In example of TC “Malware: Contagious”, major incident root causes “Patches” and “Vulnerability” were mapped to the TC. This is to represent the relationship of TC and MIC where potential malware could cause either need to patch or is spread through a vulnerability. Both categories however have resulted in major incident leading to loss of availability.

Percentage of total incidents in categories -column describes quantitatively how often the root cause of major incident appeared in the reports. In the example of TC “Malware: Contagious” the MIC “Patches” and “Vulnerability” appeared in 17% of total incidents.

Major incident multiplier -column score is calculated similarly to SOC effort multiplier and SOC multiplier. The percentage of total incidents in categories is converted to a multiplier with the same formula: 1 + MIC percentage. In example of TC “Malware contagious”, the MIC “Patches and Vulnerability” appeared 17% of times in total incidents resulting in the multiplier of 1,17. The multiplier describes how much certain major incident types in appear in the observable timeframe.

Major incident remediation (MIR)

This section contains the columns: Major incident remediation (MIR), Percentage of major incidents in categories, and Major incident effort multiplier.

Major incident remediation (MIR) describes columns represents the research data from major incidents reports containing the categorized information on how availability errors were remediated.

Percentage of major incidents in categories -columns contains MIR data in numerical format similarly as in SIC and MIC categories and describes the percentage of remediation categories appearing in total of major incident reports. In example of TC “Malware: Contagious” the related MIC “Patches” and “Vulnerability” MIR categories “Service restart”, “Server restart”, and “Patch” appeared in 24% of the total major incident reports.

Major incident effort multiplier -column uses the identical formula to other multiplier columns of MIR percentage + 1. Major incident effort multiplier describes how much certain remediation categories appear in major incident processes and can be used in conjunction with major incident multiplier to describe how much certain types of major incidents consume IT resources.

Valuation points

Valuation points -section contains only one column “Valuation points”. The point score [Vp] is calculated by combining TC sections threat points [TCp] to SOC Multiplier [SM], SOC effort multiplier [SeM], Major incident multiplier [MaIM], and Major incident effort multiplier [MIeM] resulting in a formula: TCp * SM * SeM * MaIM *MIeM = Vp.

Valuation points seek to describe how valuable processes related to certain TC, SIC, or MIC are. They combine the perceived threat level from research literature (Aljuraid and Justinia, 2022), appearance and effort from SOC reports, and appearance and effort from major incident reports.

The hypothesis is that processes that relate to remediating issues from certain TG should be valued over other if (a) the threat appears often (SM and MaIM); (b) certain remediation are done often (SeM and MIeM). TG category points guide the total result partially by giving the initial score for the multipliers which is justified since high level threats should be valued over others in consideration and presumably consumes more resources to remediate. However, if low threat score TG receives high valuation points it can be a signal that process improvements are needed to optimize the total resources.

Nevertheless, using only valuation points as a measure to valuate certain process categories over other may oversimplify the valuation process. Since the valuation points are heavily affected by

number of incidents and remediations they alone fail to describe if some part of a process needs refinement. As in, valuation points only tell what should be valued in terms of amount of work, but do not account for the actual waste and bottlenecks inside a process.

Instead, the valuation points should be compared with input from the stakeholders to analyze if same improvement areas are discovered. To enable this comparation the workshop discussion data needs to be quantified. Next chapter will discuss the quantification discussions and mapping discussion data to themes.

Table 4. Mapped threat and incident data

Threat category (TC)	Threat's Level	Threat points (TCp)	Matching SOC Incident category to threat - Enisa (SIC)	Percentage of total incidents in category	SOC Multiplier (SM)	Related SOC incident remediation (SIR)	Percentage of total remediations in categories	SOC effort multiplier (SeM)	Matching major incident category to threat (MIC)	Percentage of total incidents in categories	Major incident multiplier (MaIM)	Major incident remediation (MIR)	Percentage of major incidents in categories	Major incident effort multiplier (MieM)	Valuation points (Vp)
Malware: Contagious	Medium	2	Malicious code	11 %	1,11	Patch, Investigate, Endpoint protection	67 %	1,67	Patches, Vulnerability	17 %	1,17	Service restart, Server restart, Patch	24 %	1,24	5,37869592
Malware: Masked	Medium	2	Malicious code	11 %	1,11	Patch, Investigate, Endpoint protection	67 %	1,67	Patches, Vulnerability	17 %	1,17	Service restart, Server restart, Patch	24 %	1,24	5,37869592
Malware: Others (e.g., Ransomware)	High	3	Malicious code	11 %	1,11	Patch, Investigate, Endpoint protection	67 %	1,67	Patches, Vulnerability	17 %	1,17	Service restart, Server restart, Patch	24 %	1,24	8,06804388
Denial of service attacks	High	3	Availability	4 %	1,04	Scrubbing	3 %	1,03	Network error	13 %	1,13	Service restart, Server restart	23 %	1,23	4,46658264
Phishing	Medium	2	Information gathering	12 %	1,12	Investigate, Reset, MFA	34 %	1,34	Vulnerability	1 %	1,01	Patch	1 %	1,01	3,06193216
Masquerade	High	3	Information gathering	12 %	1,12	Investigate, Reset, MFA	34 %	1,34	Vulnerability	1 %	1,01	Patch	1 %	1,01	4,59289824
Data injection	High	3	Availability	4 %	1,04	Investigate, Configure	27 %	1,27	Database error, vulnerability	5 %	1,05	Fix configuration, Service restart, Patch	68 %	1,68	6,9896736
Hardware/software errors or failures	Medium	2	Availability	4 %	1,04	Investigate, Configure	27 %	1,27	Server error, Database error, Network error, Service error	50 %	1,50	Service restart, Server restart, Fix configuration	74 %	1,74	6,894576
Obsolete technology/out of date HIS	Medium	2	Vulnerable	65 %	1,65	Investigate, Configure, Patch	74 %	1,74	Patches, Vulnerability	17 %	1,17	Service restart, Server restart, Patch	24 %	1,24	8,3304936
Critical infrastructure or power failure	High	3	Availability	4 %	1,04	Investigate, Configure	34 %	1,34	Server error, Database error, Network error, Service error	50 %	1,50	Service restart, Server restart, Fix configuration	74 %	1,74	10,911888
Human usability error	Low	1	Other	8 %	1,08	Investigate, Configure, Reset	37 %	1,37	Misconfiguration	14 %	1,14	Server restart, service restart, Fix configuration	74 %	1,74	2,93493456

4.2.3 Workshop discussion quantitation

To apply comparation to the results of the Table 4. the workshop discussions with the shareholders must be quantified. This process translates the qualitative data of discussion into measurable numeric information.

To quantify the data the workshop discussion transcription was translated and cleaned of irrelevant information in the context of the thesis. Next a coding scheme was developed to tag the discussion data. After applying tagging to discussion data, the frequency information of each tag was collected to Table 5.

Data cleaning and translation

Workshop discussion data was first limited to the open discussion that was held after the initial presentation. After that all comments made by the author were removed. Next the data was translated from Finnish to English. Initial translation was performed utilizing AI translation tool DeepL and after that the AI translation was corrected for grammar errors by the author by cross referencing the AI translated data to the original Finnish script. Participant names, service providers and systems used were anonymized.

Coding Scheme Development

Coding scheme for the discussion data was developed utilizing Table 4 data and combining and generalizing similar categories from columns: “TC”, “SIC”, “SIR”, “MIC”, and “MIR”. This was done to create a list of potential themes and categories that might arise from the discussion data as each row from Table 4 required a way to cross examine the category appearance in the workshop discussion data. Similar categories from each row were grouped under a same tag to improve the feedback of the discussion data to the cross comparation. Following Table 5. presents the final tagging scheme and what categories were left out in result of the combination and generalization.

Table 5. Combined category data

Table 4. row number	Combined tags TC	Combined tags SIC	Combined tags SIR	Combined tags MIC	Combined tags MIR	Discarded categories used in combination and generalization
1.	Malware	Malware	Patch, Investigation, Endpoint security	Patch, Vulnerability	Restart procedures, Patch	Malware: Contagious, Malicious code, Patches, Investigate, Endpoint protection, Service restart, Server restart
2.	Malware	Malware	Patch, Investigation, Endpoint security	Patch, Vulnerability	Restart procedures, Patch	Malware: Masked, Malicious code, Patches, Investigate, Endpoint protection, Service restart, Server restart
3.	Malware	Malware	Patch, Investigate, Endpoint protection	Patch, Vulnerability	Restart procedures, Patch	Malware: Others (e.g., Ransomware), Malicious code, Patches, Investigate, Endpoint protection, Service restart, Server restart
4.	Availability	Availability	DDOS	Availability	Restart procedures,	Denial of service attacks, Service restart, Server restart, scrubbing, network error
5.	Information gathering	Information gathering	Investigation, Account security	Vulnerability	Patch	Phishing, Investigate, Reset, MFA
6.	Information gathering	Information gathering	Investigate, Account security	Vulnerability	Patch	Masquerade, Investigate, Reset, MFA
7.	Vulnerability	Availability	Investigation, Configuration management	Availability, vulnerability	Configuration management, Restart procedures, Patch	Investigate, Configure, Fix configuration, Service restart, Database error, Data injection
8.	Availability	Availability	Investigation, configuration management	Availability	Restart procedures, configuration management	Hardware/software errors or failures, Investigate, Configure, Service restart, Server restart, Fix configuration, Server error, Database error, Network error, Service error
9.	Outdated technology	Vulnerability	Investigation, configuration management, Patch	Patch, Vulnerability	Restart procedures, Patch	Obsolete technology/out of date HIS, nvestigate, Configure, Service restart, Server restart, Vulnerable
10.	Availability	Availability	Investigation, configuration management	Availability	Restart procedures, configuration management	Critical infrastructure or power failure, Investigate, Configure, Server error, Database error, Network error, Service error, Service restart, Server restart, Fix configuration
11.	Human error	Human error	Investigation, configuration management, Account security	Human error	Restart procedures, configuration management	Human usability error, other, misconfiguration, Investigate, Configure

The categories combined and generalized from table 5. were the following: Malware, Patch, Investigation, Vulnerability, Restart procedures, Endpoint security, DDOS, Availability, Account security, Information gathering, Outdated technology, Configuration management, and Human error.

Table 6. Tag categories, description, and combinations

Tag category	Generalized description	Combined from table 4 categories
Malware	Discussion related to malware and it's subtypes	Malware: Contagious, Malware: Masked, Malware: Others (e.g., Ransomware), Malicious code
Patch	Discussion related to patching operations	Patches
Investigation	Discussion related investigation done either in SOC, IT-management or by service provider	Investigate
Vulnerability	Discussion related to vulnerabilities in hardware or software that could lead to incidents in example loss of availability	Vulnerable
Restart procedures	Discussion related to operations that require or lead to server or service restart.	Service restart, Server restart
Endpoint security	Discussion related to SOC endpoint protection	Endpoint protection
Availability	Discussion related to loss of availability of services and/or data.	DDOS, Denial of service attacks, scrubbing, network error, Critical infrastructure or power failure, Server error, Database error, Network error, Service error
Account security	Discussion related to account security such as credential resets and multi-factor authentication settings	Reset, MFA
Information gathering	Discussion related social engineering tactics such as phishing or masquerading.	Phishing, Masquerade
Outdated technology	Discussion related to outdated hardware or software that does not receive security updates	Obsolete technology/out of date HIS
Configuration management	Discussion related to operations that require or lead to configuration changes on servers and services	Fix configuration
Human error	Discussion related to incidents caused by human error	Human usability error, other, misconfiguration

Table 6. presents combined tag categories that were used in quantification of the workshop discussion data. It contains generalized descriptions based on the tag category. In example if the

workshop discussion contained a sentence with discussion related to patching operations it received a [Patch] -tag.

Discussion coding and quantification

Each sentence of the relevant workshop discussion data was analyzed and tagged separately. Tags appearing multiple times on a single row in Table 5. were counted towards workshop points multiple times. The rationale for this was to give higher value to a tag score to make it more apparent that the related processes would have a wider effect on the cybersecurity operations. This was seen as justified since single issue discussed in the workshop could realistically affect multiple types of operations.

Table 7. Quantified workshop discussion data

Tag category	Tag amount	Tag points
Malware	0	0
Patch	15	1,5
Investigation	18	1,8
Vulnerability	10	1
Restart procedures	6	0,6
Endpoint security	0	0
Availability	4	0,4
Account security	1	0,1
Information gathering	0	0
Outdated technology	2	0,2
Configuration management	11	1,1
Human error	1	0,1

In table 7. the quantity of the tags is presented on the Tag amount – column. The amount was calculated using text editors search function. By searching for a "[tag]" in example "[Patch]" it revealed 15 different mentions of patching operations. In examination of the quantified workshop discussion data, it is apparent that SOC-operation related topics were not discussed almost at all. Only account security was mentioned one time. Otherwise, the discussion mainly revolved around the topics of patching, investigations, vulnerabilities, and configuration management. It can be ar-

gued that other kind of tagging system which would not produce 0 amount results would be better. The justification for keeping this tagging scheme as the quantification method is that even the SOC related threat categories from Table 4 contained multiple generalized tags shared with many other rows. In example investigations can be done either on SOC or IT-management so discussions related to investigations awarded points for SOC operations as well. The zero tag amount categories implies that SOC operations were not heavily discussed.

Tag points were calculated by dividing the tag amount score by 10. In example Patch – tag would award 15 / 10 = 1,5 points per tagged sentence in workshop discussion data. The justification behind this is that this will enable us to better perceive where shareholders see that there could be room for process improvements and what is generally seen as valuable topic in IT-operations. In that context, a topic that was mentioned multiple times should award more points than a topic that was mentioned only once. The divider of 10 was seen reasonable as it brought the workshop data scores closer to Table 4 valuations points allowing for more accurate comparison between them.

Workshop quantified data comparison

In this section we analyze the results from Table 4. and the quantified workshop data to examine if there are major deviations in valuation of different threat categories between them. Valuation based on the points is described in the next chapter. The compared points are presented in Figure 11.

Figure 11. describes the valuation gained from the developed calculation formula behind Table 4. scores, valuation gained from workshop discussion data by utilizing the coding scheme this thesis developed and the average points of the valuated data. Figure 10. contains columns named after the threat categories from Table 4 on X-axis, point amount on Y-axis, and the corresponding lines for valuation points, tag points, and point average.

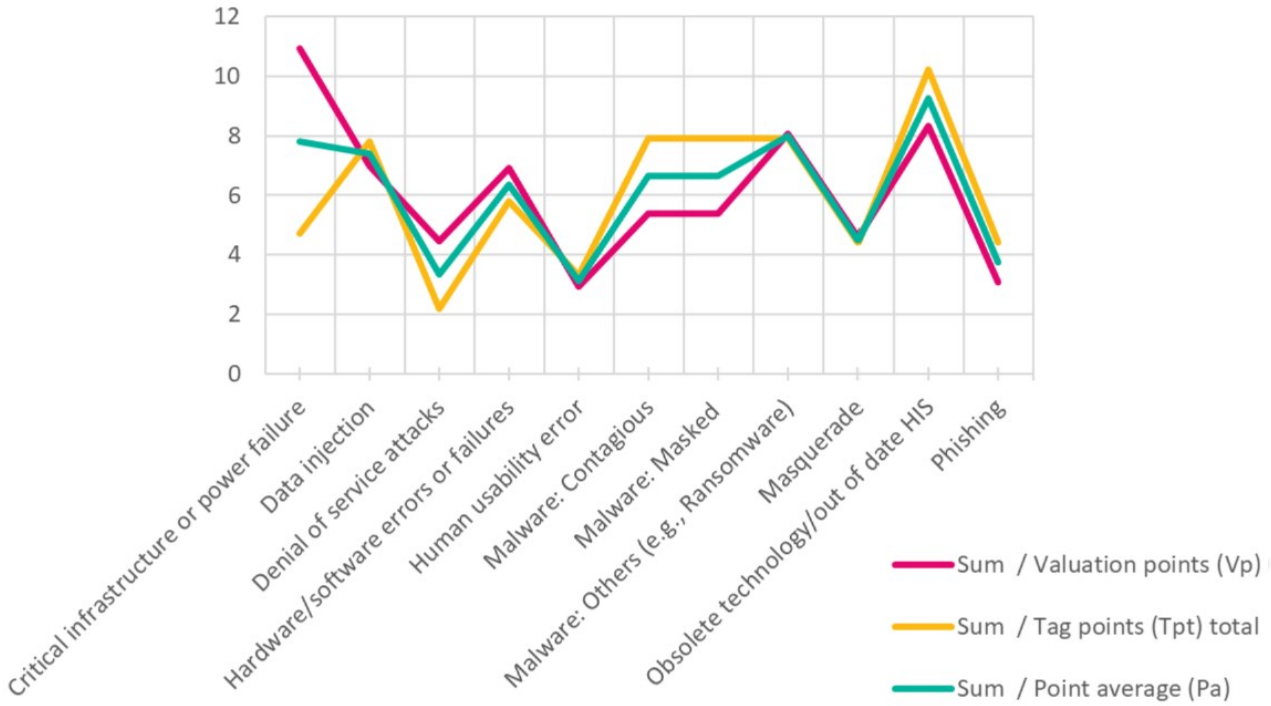

Figure 11. Valuation points vs. Tag points sum comparison.

While Figure 11. provides favorable presentation for visual comparison it is more straightforward to compare the categories using numerical data. For this reason, the same data is represented in the following table 8. with rows sorted from largest point average amount to smallest.

Table 8. Numerical comparison of valuation and tag data

Category	Valuation points (Vp)	Tag points total (Tpt)	Point average (Pa)	Avg. deviation from Pa	Vp & Tpt difference
Obsolete technology/out of date HIS	8,3	10,2	9,3	0,95	-1,9
Malware: Others (e.g., Ransomware)	8,1	7,9	8	0,1	0,2
Critical infrastructure or power failure	10,9	4,7	7,8	3,1	6,2
Data injection	7	7,8	7,4	0,4	-0,8
Malware: Contagious	5,4	7,9	6,6	1,25	-2,5
Malware: Masked	5,4	7,9	6,6	1,25	-2,5
Hardware/software errors or failures	6,9	5,8	6,3	0,55	1,1
Masquerade	4,6	4,4	4,5	0,1	0,2
Phishing	3,1	4,4	3,7	0,65	-1,3
Denial of service attacks	4,5	2,2	3,3	1,15	2,3
Human usability error	2,9	3,3	3,1	0,2	-0,4

Table 8. also includes the average deviation from Pa of Vp and Tpt. This column describes how much the valuation gained from the calculation formula used in Table 4. and quantified workshop data deviate from each other. It can be calculated by measuring the distance of Vp and Pa, distance of Tpt and Pa, adding the distances together and dividing the sum by 2. Higher deviation implicates that there is difference on how a threat category and related operations are perceived through valuation gained from Table 4. formula and how it is perceived by stakeholders in Table 7 and Table 8. The average deviation in Table. 8 is 0,88 rounded to two decimal places implicating that any deviation higher than that indicates above normal difference in perception of threat category valuation between the stakeholders and thesis data. In example critical infrastructure of power failure is seen as a highly valuated threat category in Table 4. data, but instead based on the tagged data from workshop discussions the availability loss due to this kind of root cause is not perceived as highly valuated.

Lastly Vp & Tpt difference column describes the numerical difference between valuation points and tag points. It is simply calculated with the formula: Vp – Tpt = difference. This value is another way to describe the relation between this thesis perception on threat category valuation and stakeholder valuation. Negative values represent situation where stakeholders valuate a threat category and related operations more than this thesis has valuated it with its valuation formula in Table 4. Positive values describe the opposite situation where this thesis valuates a threat category higher than the stakeholders.

4.2.4 Value assessment

Based on earlier analysis of the data it can be theorized that a threat category is valuable candidate for process development if: a) it has high valuation using the thesis valuation formula, b) it has high valuation using the developed tagging formula, indicating that the threat category is either great threat to healthcare environments and/or involves a lot of resources to mitigate.

Additionally, categories can be analyzed using the descriptive columns of Table 8. by looking at the average deviation and point difference column values. The data from descriptive columns should not be used primarily for category prioritization but instead used as additional information on where to further troubleshoot why the valuation differs from the valuation formula. In example if the case organization stakeholders tagging data valuated a threat category notably higher than the

valuation formula it could indicate that mitigation processes of the category might have problems that call for process improvements.

Utilizing the Table 8. data five different categories can be derived: Highest Vp, Highest Tpt, Highest point average, highest average deviation, and highest difference. For this thesis deviation and difference will be combined into single category.

Highest valuation points

As described earlier valuation points describe the value gained from utilizing the valuation formula developed in this thesis. High valuation points indicate:

a) high theoretical threat value based on the study of Aljuraid and Justinia, indicating that the threat category has been perceived challenging in other healthcare environments,

b) high resource utilization based on the data of SOC reports and Major Incident log data, indicating that the category uses a lot of resources of the organization.

The category with highest valuation points is Critical infrastructure or power failure. According to Table 5. this category relates most strongly to the availability of services.

Highest tag points

Tag points represent the amount in which threat category related operations were mentioned in workshop discussion data. Tag points provide a generalized view to what the stakeholders saw as valuable. High tag points indicate that:

a) threat category related processes contain problem points, indicating the processes should be analyzed for Lean process improvement cases,

b) threat category related processes utilize high amount of case organization resources, indicating that the processes could benefit from Lean improvements to optimize resource utilization.

The category with highest tag points is Obsolete technology/out of date HIS. According to Table 5. this category relates most strongly to patching operations and mitigation of vulnerabilities.

Highest point average

Highest point average represents the average of valuation points and tag points. It gives a general description of how valuable a threat category is. It combines the threats theoretical criticality and resource utilization to what the stakeholders perceive as valuable. High average point amount is well used as a general guidance on what categories to focus on. The category with highest average points is Obsolete technology/out of date HIS. Combined with the result of Obsolete technology/out of date HIS obtaining the highest tag points this evidence strongly supports it as the strongest candidate for process improvements.

Highest average deviation an VP & Tpt difference

These categories represent how much the perception of valuation data differs from the stakeholder data. VP & Tpt difference is another way of representing the same data, but it provides an additional data point depending on if the points are positive or negative. This data is unobtainable from average deviation. Negative points represent a situation where the stakeholders valued certain process related operations more than the data gained from valuation formula. Positive points describe a reverse situation where process related operations where valuated higher with the valuation formula than the stakeholder data. High deviation or difference indicates that the case organization perceives a threat category differently than the valuation formula; in such case it may be valuable to analyze are the mitigation processes and controls already in place sufficient.

Based on previous analysis of this thesis, if threat category receives high valuation from formula but has high difference it could indicate that there may not be sufficient controls in place. If a threat category receives high valuation from stakeholders but there is high difference it could indicate that there are problems within the processes. The category with highest deviation and difference points is Critical infrastructure or power failure. According to Table 5. this category relates most strongly to operations related to availability of services that are not part of the configuration management in example sudden power outage.

Most valued threat category

Based on the value assessment of different threat categories the top place for most valued category is tied between "Critical infrastructure or power failure" and "Obsolete technology/out of date HIS".

Critical infrastructure or power failure had the highest Vp, average deviation, and difference indicating that it is highly valued threat utilizing the formula of Table 4. However, in stakeholder workshop processes related to mitigating availability losses due to sudden infrastructure or power failures were not discussed frequently. This manifests in the high deviation and difference scores. High deviation and difference could indicate that the threat category related operations are not valuated enough by stakeholders, but it can also indicate that the operations were not discussed since well working processes are already in a place such as regularly maintained uninterruptible power supplies in core services and clustered servers. Also due to the nature of threat category being related to sudden or unexpected challenges in services discussions related to it may not surface naturally without guidance.

Obsolete technology/out of date HIS had the highest Tpt and point average with moderately low deviation and difference indicating that stakeholders observed problems with related processes and that the threat category was similarly valuated using the Table 4. formula. The moderately low deviation and difference indicate that the workload utilization of this category is correctly perceived by both the valuation formula and the stakeholders.

Ultimately the decision between the two categories had to be made. Should we value perceived threats from academic literature in reference to higher threat level categorization of "Critical infrastructure or power failure", or should we value the stakeholders opinion on process challenges relating to "Obsolete technology/out of date HIS"? Since this thesis is a case study that utilizes Lean methodology to improve processes a personal choice was made to choose "Obsolete technology/out of date HIS" as the improvement category. This is justified as it applies the principle of respect for the people by valuing the experiences of the stakeholders and the organization higher than the theoretical threat level of "Critical infrastructure or power failure".

4.2.5 Organizational controls

To apply optimizations to processes related to Obsolete technology/out of date HIS -category, organizational controls, or lack of, related to them need to be identified. Organisational controls related to the chosen category could be in example: regular inventory checks, risk assessments, ensuring compliance, enhanced security measures, change management, and vendor management.

To keep this research in scope we will not be exploring all the processes behind all possible controls. Instead, we'll inspect the controls most closely related to the SIC, SIR, MIC, and MIR categories from table 5. which can be divided into two subcategories under SOC-operations and IT-management operations. In general SOC-operations consist of work done to detect, prevent and mitigate cyberthreats. IT-management operations in this regard are more related to the maintaining of the availability of the service via configuration management, patching and restart procedures via ISMS controls and processes behind them.

Table 1. describes the motive for the category as "usually unintentional, often resulting in untrustworthy and unreliable systems" suggesting that out-of-date systems usually are left operational unintentionally and since they either are not up to latest security standards or cannot be patched, they are deemed untrustworthy and unreliable. This can be a serious problem if the system contains sensitive patient information endangering the confidentiality, integrity, and availability of important data in case of a breach.

Specific to this category the incidents that SOC detects are related to vulnerabilities in out-of-date technology. In example SOC can detect a new 0-day vulnerability affecting a specific subset of systems. To remediate these issues SOC performs investigations to possible vulnerable systems, informs related IT-teams of the vulnerability and describes possible workarounds and fixes for the vulnerability. In case of a major incident such as a 0-day affecting servers that contain sensitive information the remediation has been a joint-operation between SOC and IT-management under the major incident management process.

The workshop discussions with stakeholders revealed significant challenges in the processes related to the acquisition of assets, particularly concerning their possible inherent weaknesses regarding information security. These challenges emphasize the importance of process challenges

throughout the asset acquisition lifecycle. In this context to gain answer to the RQ1: “What processes in their ISMS the case organization should improve to enhance their cybersecurity?”, it must be first assessed which controls are deployed to mitigate unintentional out-of-date systems in organizations environment, and what is being done to control the systems availability. Based on the earlier research data and workshop discussions the focus on process improvements should be on processes behind controls that the organization has deployed regarding IT-acquisitions and securing their availability.

4.2.6 Acquisitions and information security requirements

In adherence to organizational policy, the IT management serves as the sole acquisition channel for computers, IT licenses, and services. Users initiate acquisition requests by emailing the IT management service. Furthermore, the organization imposes two types of information security requirements on systems based on their handling of patient data. If patient data is involved, a data protection impact assessment must precede system implementation into the production environment.

Acquisitions

The organizational acquisition guide delineates three categories: small-scale acquisitions (under 60,000€), national-scale acquisitions (over 60,000€), and EU threshold-crossing acquisitions. Small-scale acquisitions are exempt from competitive bidding under acquisition laws. For clarity in this thesis, we'll categorize acquisitions as either bid or non-bid.

Aligned with the internal policy on acquisition channels, IT management must be contacted before accepting any network-connected device or service acquisition. Sufficient time must be allotted for IT management to assess and provide feedback, especially if the acquisition surpasses the bidding threshold.

Bidding petitions must detail selection and evaluation criteria. Tenders are to be chosen solely based on these criteria, prioritizing the most economically advantageous tender. Criteria may include lowest price, cost-effectiveness (including life-cycle costs), or the best price-quality ratio.

Clear minimum requirements justify competitive bidding based on the lowest price, while quality criteria encompass technical, aesthetic, and functional aspects, accessibility, and user needs.

Regarding acquisitions involving personal data handling systems, GDPR mandates an agreement on data processing between the organization and the provider. The agreement outlines respective duties and responsibilities, emphasizing its consideration during acquisition planning. Before integrating the new service or device into production, a Data Protection Impact Assessment (DPIA) is obligatory.

Information security requirements

Two essential documents, denoted as Type A and Type B information security requirements, form the backbone of bidding processes within our procurement framework. Each document outlines fundamental security protocols and obligations for our suppliers, ensuring the integrity and protection of sensitive data. Incorporated into bidding procedures, these documents serve as definitive guidelines, shaping the criteria against which potential suppliers are evaluated and selected.

Type A information security requirements define stringent protocols and standards that the service provider must adhere to in order to ensure the confidentiality, integrity, and availability of organizations sensitive data and systems. These Type A requirements encompass organizational and physical security measures, user authentication protocols, data encryption standards, continuity planning, and collaboration for audits and security clearances.

Type B requirements describe the fundamental security requisites binding the Supplier, emphasizing the safeguarding of data integrity and confidentiality within the context of their contractual obligations to Fimlab. It establishes a framework for ensuring that the Supplier's systems, services, and facilities meet minimum security standards, encompassing both physical and digital realms. Additionally, it outlines procedures for risk mitigation, access control, incident reporting, and post-contract data handling.

Difference between the documents is that type A requirements encompass foundational security measures necessary for safeguarding sensitive data and systems. These may include protocols for organizational and physical security, user authentication, data protection, and basic continuity planning. Type A requirements serve as fundamental elements to ensure a minimum level of security compliance. Conversely, Type B requirements are less restrictive. They cover essential aspects of security but with fewer restrictions compared to Type A. This differentiation allows for flexibility in addressing varying levels of risk and compliance needs.

4.2.7 Value stream mapping

Value stream mapping is used to visualize and analyze the steps involved in delivering a product or service from start to finish. When applied to acquisition and deployment processes, it provides an overview of the process, from identifying the need for a product or service to its successful implementation. By mapping out each step in the process, including interactions with suppliers, internal approvals, and deployment procedures, organizations can identify inefficiencies, bottlenecks, and areas for improvement.

Acquisition value stream

The acquisition value stream illustrates the sequential stages and subprocesses needed to acquire a new IT service or asset. It depicts the journey from identifying the need for acquisition to the final deployment or integration of the acquired entity into the existing system or infrastructure. Acquisition value stream map provides a visual representation of the existing workflow, highlighting the sequence of activities and handoffs between departments or individuals. Value stream for acquisitions is represented in Figure 12. In the context of the case organization and this thesis work, the value streams derived from the processes do not emphasize process time metrics but rather focus on representing each process step and delineating the responsibilities of the actors involved. This approach prioritizes understanding the flow of activities and the roles and interactions of individuals within the organization.

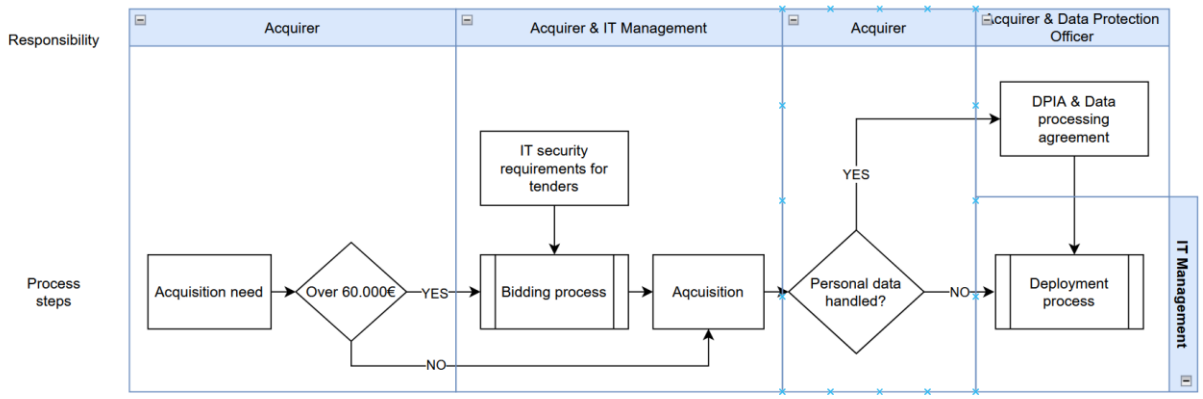

Figure 12. The acquisition value stream

Inefficiencies and bottlenecks identified in the current state will be further discussed and analyzed in the next chapter. These discussions will focus on understanding the root causes of these issues and developing strategies to address them, ultimately aiming to optimize the workflow for improved performance and outcomes.

Deployment value stream

The deployment value stream outlines the process from acquisition or development completion to final implementation in the production environment (Figure 13.). It includes tasks such as testing, configuration, installation, and user training. This map also incorporates essential elements like setting up virtual servers, vendor service connections, and firewall configuration.

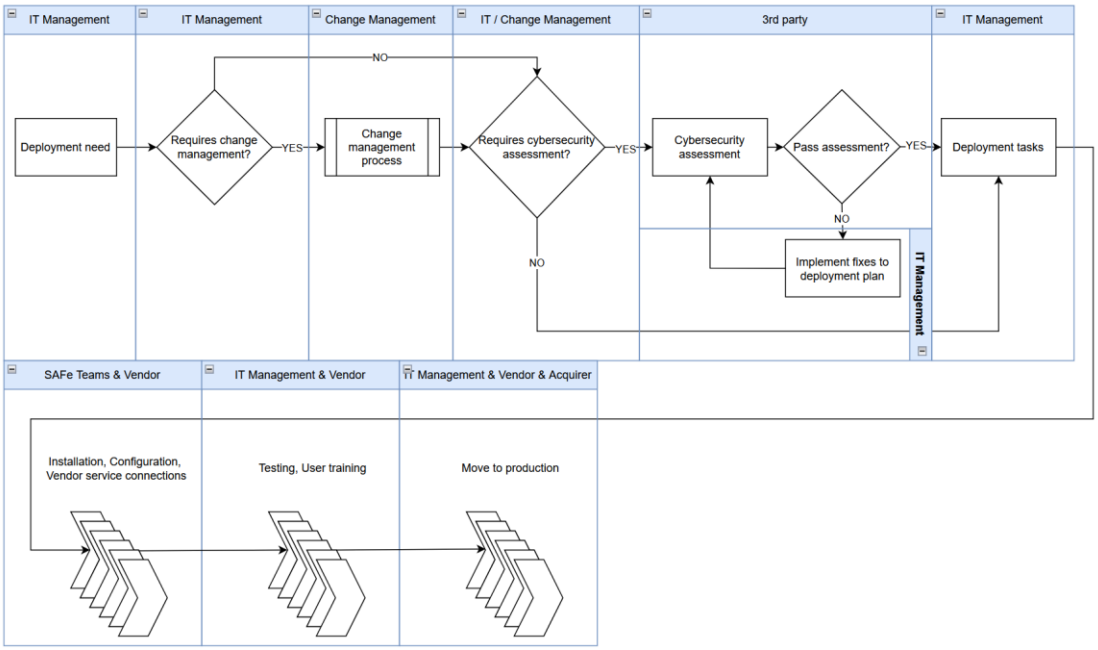

Figure 13. The deployment value stream

Currently, this value stream reflects operations within the Pirha environment. However, as part of an ongoing ICT transition project, the organization is transitioning towards its own environment. Given the dynamic nature of this transition, processes within the value stream are subject to change. It serves as a blueprint for understanding the sequence of activities involved in deploying solutions and systems.

Bottlenecks and challenges

In this section, the bottlenecks and challenges encountered within the acquisition and deployment value streams are identified and analyzed. The aim is to develop insights and strategy to overcome them to optimize the processes. Based on the workshop discussion research data and authors personal experience, several bottlenecks and challenges hinder smooth operations within acquisition value stream. One significant issue arises from acquirers' uncertainty regarding which information security requirements to apply. This ambiguity often results in the purchase of assets lacking adequate security measures, complicating subsequent security assessments and deployment processes (to be further addressed in the deployment phase). Additionally, delays in Data Protection

Impact Assessments occur due to insufficient information and unclear responsibilities. These challenges impede the timely and efficient acquisition of new assets and highlight the need for clearer guidelines, enhanced communication, and streamlined processes within the acquisition value stream. The authors personal experience observed challenges regarding the lack of knowledge or unclear responsibilities regarding DPIAs, as well as uncertainties regarding the necessity of change management for asset deployment. The authors personal experiences will be further validated in the workshop feedback section of the Results chapter where a second workshop with the shareholders is held to validate thesis results.

Based on the workshop discussion research data and authors personal experience, the following challenges in deployment value stream can be identified. One notable difficulty arises from uncertainty surrounding the necessity of change management protocols, potentially leading to delays and confusion during implementation. Additionally, cybersecurity assessments often consume excessive time, repeating evaluations of the same elements and prolonging the deployment process unnecessarily. Another difficulty involves the lack of clarity regarding how to fix issues identified in the deployment plan during the cybersecurity assessment, further hindering progress and causing delays. Addressing these challenges is crucial for streamlining deployment procedures and ensuring efficient workflow that enabled agile deployment into operational environments.

Improvement strategies for challenges

Recognizing challenges inherent in the acquisition and deployment processes, this section explores the approaches aimed at streamlining processes, enhancing cybersecurity measures, and optimizing resource utilization.

To streamline the acquisition process, it's essential to align IT security requirements ensuring that the organization has a clear understanding of its technological needs, budgetary constraints, regulatory compliance requirements, and stakeholder expectations. Organization should perform a comprehensive review of existing security requirements to identify potential gaps or vulnerabilities, and the formulate an updated security requirements to address emerging threats.

Since the requirement to perform a data protection impact assessment (DPIA) is tied to the question if personal data is being handled, the impact assessment could be tied to the security assessment based on similar criteria. This would bring structure and standardization to the work process and could ensure timely execution of the DPIA. Furthermore, enforcing the use of these revised requirements, by instituting strict adherence to security protocols throughout the acquisition process, organization can mitigate risks associated with acquiring outdated technologies and enhance overall resilience against cyber threats.

IT security requirements should be seamlessly aligned with deployment processes that follow best practices. These practices can be templated into tasks for development teams, ensuring that security considerations are integrated throughout the development lifecycle. During security assessments, if a feature is found to be non-compliant with these aligned requirements, a special task is generated in the change management process instead of blocking deployment. In this task the deficiencies are accounted for, and other layers of security added such as, firewalls, antivirus software, intrusion detection systems, and encryption protocols to protect data integrity and confidentiality. This approach facilitates the resolution of security issues without impeding progress and minimizes redundant security evaluations.

Additionally, encouraging collaboration between cybersecurity and deployment teams is essential for clarifying and resolving issues identified during assessments. Establishing cross-functional teams and using open communication channels can help the resolution of deployment plan issues on time, preventing unnecessary delays and ensuring smooth progress throughout the deployment process.

Strategies for existing out-of-date assets

Organization should conduct regular inventory checks to identify all obsolete technologies and out-of-date components within the organization. This proactive approach ensures comprehensive awareness of the IT landscape, enabling effective planning and decision-making. Acquired systems containing technology that is outdated or against the requirements should be monitored with special detail on anomaly detection mechanisms to identify unusual behavior or patterns that may signify compromise, such as detecting unexpected network traffic, unauthorized access attempts,

or abnormal system activity. Setting up the monitoring should be a mandated task for deployment teams after security assessment has identified outdated technology. This demands new process for IT management, development team and SOC co-operation.

Vendor relationships and contracts associated with outdated technology or obsolete Health Information Systems (HIS) should be evaluated. Engage in negotiations with vendors for support, maintenance, or upgrade options. If necessary, explore transitioning to alternative vendors to ensure continued support.

5 Results

This chapter presents the outcomes of applying lean methodologies within the context of cybersecurity processes related to acquisition and deployment of IT-assets. It presents the application of Lean methods aimed at refining incident response processes. Additionally, it presents the envisioned future state value streams. Future state value streams are evaluated through a workshop with stakeholders where the effectiveness of the proposed future state processes is assessed. Stakeholder feedback, areas of acceptance, and opportunities for improved efficiency in cybersecurity operations are represented.

5.1 Applying Lean methods

After assessing most valuable processes for optimization following Lean methods were applied to improve cybersecurity process efficiency.

Value stream mapping was used to lay out the processes related to selected controls. Value stream maps describe the process steps used to reach the final value of the process. In this thesis also the responsibilities of different inter and extra organizational parties were mapped to process steps. The value stream map was developed to provide a comparation point to the future state value stream maps in which process optimizations are applied.

Continuous improvement (Kaizen) was implemented by integrating feedback loops at the end of processes. These loops are used to capture insights on current process efficiency and gather suggestions for improvement. Feedback from stakeholders and team members can be used to optimize cybersecurity practices, ensuring ongoing improvement.

Cross-functional collaboration is fostered by incorporating additional process steps after deploying monitoring for IT management, development, and SOC teams. This integration ensures that relevant stakeholders from different departments are involved in monitoring out-of-date systems for anomalies.

Work standardization is achieved by incorporating information security requirements and cybersecurity assessment outcomes into the templating of development tasks. This ensures that all development activities adhere to established security standards and best practices, reducing the risk of vulnerabilities, and enhancing overall cybersecurity posture. By standardizing tasks based on security requirements, organizations can streamline development processes and minimize security risks associated with system deployment. The addition of templated deployment tasks also eliminates the process halting loop of cybersecurity assessments. In the future state the deployment will be able to move forward even if the acquired asset fails the assessment.

5.2 Future state value streams

In this chapter the future state acquisition and deployment value stream is described. Detailing a comprehensive walkthrough of the entire process. The aim is to provide a detailed explanation of how the future state of these value streams will operate, from the initial acquisition phase to the final deployment into the operational environment. By offering a step-by-step walkthrough, readers will gain a thorough understanding of the envisioned process and how it aligns with organizational goals and objectives. This detailed exploration will shed light on the improvements and optimizations that have been made to enhance efficiency, reliability, and effectiveness in both acquisition and deployment processes. Figure 14. depicts the future state value streams of acquisition and deployment processes.

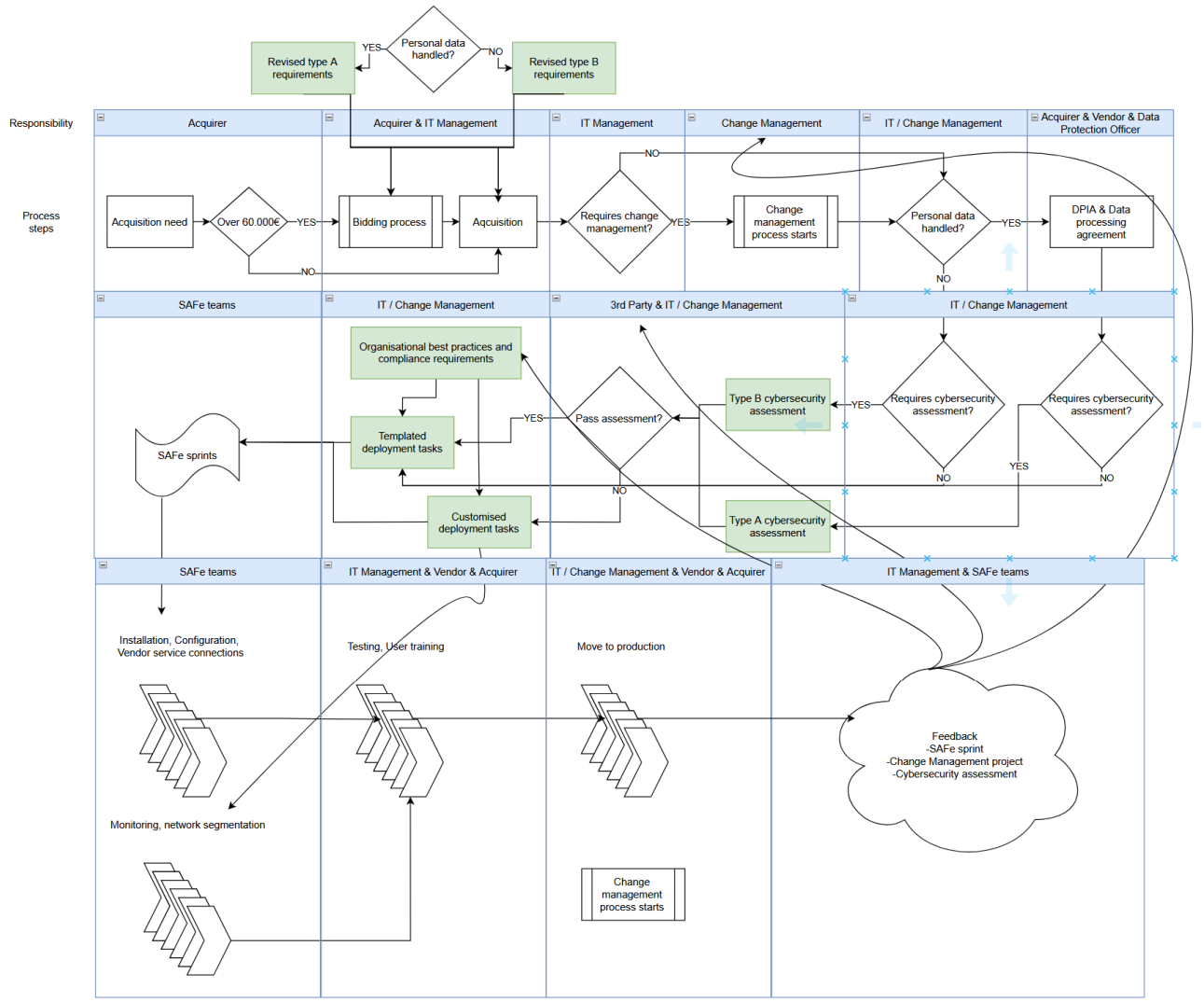

Figure 14. Future state acquisition and deployment processes

Process walkthrough

In Figure 14. the whole chain of process steps is visualized. The process starts with the acquisition need of a department. The acquirer assesses the acquisition for the need of bidding. If the acquisition is over 60.000€ in value it needs competitive bidding. In both cases the acquisition is subjected to Type A or Type B security requirements depending on if personal data will be handled by the acquisition. Collaboration between the acquiring party and IT management facilitates a review of these requirements, with IT management also evaluating the need for a change management process, especially for entirely new assets. Next data protection impact assessment is performed if

the acquisition involves the handling of personal information. Third-party service providers carry out Type A or Type B cybersecurity assessments based on predetermined criteria.

Upon meeting the requirements, the asset progresses to the deployment phase, where templated deployment tasks are assigned to SAFe teams' backlogs. In the event of cybersecurity assessment failure, IT or change management devises customized deployment tasks to address information security deficiencies. SAFe teams will then handle the deployment tasks in their work sprints and testing and user training will be organized in co-operation by IT Management, asset vendor, and the acquiring party.

Once testing and user training are completed, the asset is prepared for deployment into the production environment, a task that involves scheduling and coordination among stakeholders. Change management or IT management oversees the move to production, depending on whether the deployment required the change management process. Feedback is collected at the end of the process, encompassing change management procedures, cybersecurity assessments, and the performance of deployment teams. This could include feedback on the execution of deployment tasks, adherence to timelines, and effectiveness in achieving deployment objectives. SAFe teams have built-in processes for this kind of retrospective but change management and security assessment processes do not. This could be resolved by establishing change management team and cybersecurity assessment team that would follow these same principles.

5.3 Evaluation of suggested future state processes

To evaluate the future state value streams a workshop was held with the same stakeholders from earlier process workshop. The controls and processes chosen were discussed and the description of current state processes was assessed for valid description. Suggested future state value streams were displayed and feedback was gathered if they were seen as potential alternative for current state. In addition, further development needs were discussed. Workshop discussion was recorded to provide accurate statements for the feedback sections.

Workshop feedback

Workshop stakeholders were briefed on the logic and methodology behind the selection of acquisition and deployment processes. Selection method based on comprehensive study data, including analyses of SOC incidents and the major incident calendar was explained. Overall, stakeholders expressed agreement on the value and relevance of the chosen processes. When presented with the current state value streams the stakeholders agreed that the descriptions of the current state value streams were accurate. They acknowledged that the acquisition and deployment process steps contained all the core activities related to acquisition and deployment process.

The challenges and bottlenecks highlighted in the current processes were unanimously acknowledged during the workshop. These challenges contained both the issues identified in the earlier process workshop and the personal observations of the author. Personal observations and challenges perceived from the earlier process workshop were differentiated clearly to the stakeholders to separately gain validation to them. The stakeholders recognized the importance of addressing these challenges to streamline the acquisition and deployment process.

Future state processes were generally acknowledged as potentially valuable by stakeholders. Additionally, stakeholders offered several suggestions for further development. The stakeholders emphasized the need to align cybersecurity assessments to organizational environment and the role of change management. System ownership from a risk management perspective, was also discussed. A key idea was to define clear ownership roles for new systems early on to ensure strong commitment from owners to cybersecurity assessments and DPIA. Defining ownership was seen possible through an additional process step conducted before DPIA evaluation. Utilizing templates as part of the deployment process was seen selectively valuable. Not all features of deployment tasks were deemed suitable for templating. However, leveraging templates in deployment could offer additional assistance in streamlining the process, especially for complex systems. One of the main conclusions emphasized the importance of setting precise requirements, especially regarding data protection and security.

Generally, the workshop proved valuable in validating the research and development conducted in this thesis. The acceptance of the potential value of the proposed future state value streams by

stakeholders validated the significance of the work undertaken and its relevance to addressing organizational challenges in cybersecurity processes.

5.4 Addressing the research questions

This chapter provides a summary of the findings obtained in this thesis work in response to the research questions posed. Through analysis of various data sources and stakeholder engagements, the research questions have been systematically addressed to provide valuable insights into enhancing cybersecurity practices within the organization.

-RQ1: What processes in their ISMS the case organization should improve to enhance their cybersecurity?

-RQ2: What are the specific problem points that can be solved and improved upon?

-RQ 3: How to apply lean thinking to ISMS processes?

-RQ 4: How to implement these processes?

To answer RQ1 on what processes the case organization should improve upon was answered through analyzing the workload and challenges presented by various threat categories. By assessing valuation and workshop discussion scores to each category the most valuable category of processes was systematically chosen. Through selection of the category “Obsolete technology/out of date HIS” the controls related to it could be assessed. To maintain the research within scope, not all controls were investigated for development. Instead, the focus was on controls and processes related to the acquisition and deployment of IT assets. The justification for chosen controls was based on process workshop discussion where multiple challenges were identified directly related to these controls.

In RQ2 the specific problem points associated with the selected controls and processes were identified through workshop discussions and personal experience gained from these processes. The current state of the processes was represented as a value stream to clearly define the process steps and responsibilities. This personal experience was validated during a subsequent workshop

with stakeholders, and the challenges identified within the value stream were unanimously agreed upon. These challenges were identified within the acquisition and deployment phases:

Acquisition:

1. Uncertainty regarding which security requirements to apply in asset acquisitions.
2. Acquisition of outdated or otherwise insecure assets.
3. Challenges related to Data Protection Impact Assessments (DPIA), including a lack of knowledge or unclear responsibilities.

Deployment:

1. Uncertainty regarding the necessity of change management for asset deployment.
2. Length of cybersecurity assessments.
3. Addressing issues identified during cybersecurity assessments.
4. Repetitive evaluation of the same aspects across multiple assessments.

The application of Lean thinking to the selected ISMS processes in RQ3 contained value stream mapping to visualize and analyze both the current and future states of the chosen processes. This mapping helped identify inefficiencies, bottlenecks, and areas for improvement. Secondly, continuous improvement principles were applied by introducing an additional feedback step at the end of the value streams. This feedback loop allowed for insights and suggestions to be captured from stakeholders and end-users, facilitating ongoing refinement and enhancement of the processes. Cross-functional collaboration was facilitated by integrating additional process steps to deployment phase to ensure involvement and coordination among IT management, development, and SOC teams. This approach aimed to enhance communication between different teams. Work standardization was implemented by introducing the concept of deployment templates and by suggesting revising of the cybersecurity requirements to ensure consistency and clarity across processes.

The implementation of the future state processes in RQ4 was showcased to stakeholders through future state value streams, providing a clear visual representation of the proposed processes. During the second workshop, stakeholder feedback validated the process model, confirming its applicability and effectiveness in addressing the identified challenges. This approach also enabled the

refinement of the proposed processes for optimal efficiency and efficacy through additional development feedback from stakeholders.

6 Conclusions

This thesis research provides valuable insight into the development of Lean cybersecurity processes for the case organization. By applying Lean methodologies, significant improvements in efficiency, effectiveness, and agility have been proposed. The findings of this research benefit not only the case organization but also offer valuable lessons and strategies for other organizations seeking to enhance their cybersecurity processes.

Implications of the research

The conducted research has several implications. Firstly, it displays the effectiveness of applying lean methodologies to ISMS processes, describing how Lean methods can streamline cybersecurity practices. Secondly, the research reveals the importance of stakeholder involvement and feedback in optimizing processes. Additionally, the research demonstrates the significance of identifying and addressing specific problem points within ISMS processes. Overall, the findings suggest that adopting lean principles to processes is plausible and can lead to more efficient, resilient, and secure cybersecurity practices within organizations.

Further development and research

The research identified several areas for further development and exploration. One aspect is enhancing the threat category value calculation framework by integrating teams cybersecurity related activities into the same work platform and implementing consistent tagging of work activities thus eliminating manual labor surrounding translation of team activities to categories. This integration would enable continuous improvement and regular reviews of workloads that utilize team resources, thereby ensuring the up to date and accurate threat category workload information.

Another area for development involves the bidding processes, specifically in relation to IT security requirements and their application. Organizations should aim to quantify the costs associated with implementing deficient systems, thereby enabling better evaluation of tenders, and assisting in the elimination of insecure assets acquisitions.

Future research could explore methods for gathering feedback at various stages of the process without disrupting workflow. This could involve investigating techniques for seamlessly integrating feedback mechanisms into existing processes, such as implementing automated feedback loops or utilizing specialized software tools. Additionally, research could focus on identifying optimal timing and channels for collecting feedback to ensure it is timely and relevant. By addressing these aspects, future studies could provide valuable insights into enhancing feedback collection practices and ultimately improving process effectiveness and efficiency.

7 Discussion

This chapter discusses the reflective analysis of the thesis research, assessing if the research goals of the thesis were met. It explores the challenges identified in the research process related to methodological and practical challenges. Ethical considerations are discussed, relating to integrity of the research. Additionally, the quality of the research outcome is evaluated. Through this reflection the aim is to provide a comprehensive evaluation of successes and areas for improvement.

Reflection

The research was able to answer the research questions, providing insight into the chosen topic. The obtained results gained acceptance within the case organization stakeholders, suggesting relevance and applicability of the research findings. This reflects positively on the applied research methodology. In the context of research data the results were expected, appliance of Lean methodology is a viable strategy to streamline processes and cybersecurity is not an exception.

Limiting factor in the research is the amount of data used in the research. Similar research would benefit from longer period of data collection and standardized tagging of work categories. Another limiting factor was the size of the workshop group of the stakeholders. Feedback would be more

comprehensive if the workshop group would have been larger and included specialists from multiple teams. Although workshop is a valuable way to gain information and feedback from stakeholders, the scheduling and organizing becomes more difficult as the number of people increases providing challenges to the research conducted.

This research holds beneficial implications for organizational practices and policies. By identifying and addressing challenges within the acquisition and deployment processes, organization can enhance their cybersecurity posture and operational efficiency. It also provides a foundation for further development in developing the controls related to the IT asset lifecycle. Based on the findings and methodology presented in this study, organization could focus their resources to improve controls and processes related to asset maintenance, monitoring, and decommissioning of IT assets.

Challenges

In this section the challenges encountered throughout the research are explored. Despite preplanning of the thesis work, few unpredicted obstacles arose that required adaptation of the research methodology and applying problem solving.

Excluding the category "Management weakness" from the original study by Aljuraid and Justinia (2022) was a decision based on its perceived lack of relevance to the analysis of SOC and MIM processes. The category is characterized by management shortcomings resulting from factors such as staffing and budget constraints or lack of experience, was suspected to be challenging to map to either SOC or MIM controls. Additionally, it was determined that including this category would not contribute to the analysis of the processes underlying the controls.

During the workshop discussion coding, it became clear that many discussion tag categories contained interconnected work, leading to challenges in assigning the discussion tags to individual threat categories in Table 7. They presumably contain spillover work related to other threat categories. Spillover work in this context refers to the additional tasks or efforts required to implement specific controls or processes. The consideration of spillover work reduces the accuracy of assessing the effect of various tag categories on the value comparison of the threat categories. A different coding scheme could have affected on the selection of the threat category.

On the contrary selection process was only part of the research and optimization methods explored in this research can be applied, nevertheless. It could be beneficial to refine the quantification methods to ensure comprehensive consideration of all related factors to obtain improved understanding of the resource utilization of threat categories within the organization.

Ethical considerations

In considering ethical implications, it's important to acknowledge that while the Prisma review provided a structured approach, its domain percentages didn't fully capture the breadth of literature reviewed for the thesis. As the research progressed, it became apparent that cybersecurity frameworks weren't as relevant as initially anticipated. Additionally, the literature review alone couldn't offer all the required insights, necessitating the supplementation of knowledge from singular sources to adequately provide relevant information related to the research subject.

Additionally, the workshop discussion data can exhibit a degree of bias due to the predefined topics set in the meeting agenda, which may constrain the scope of conversation. To mitigate this limitation and to capture a wider range of feedback, a follow-up study employing open-ended questions in interviews could offer valuable supplementary information.

Research ethics were considered in the utilization of personal work experience during workshop discussions and the identification of challenges. The decision to incorporate personal experiences was made with consideration to ensure transparency and integrity in the process. Validation of these personal experiences was sought from stakeholders within the case organization stakeholders, thereby validating the credibility and reliability of the findings. However, it is important to acknowledge the potential bias that may arise from being a member of the case organization, as it could influence perceptions and judgments.

References

Alblooshi, M., Shamsuzzaman, M., Chong Khoo, M. B., Rahim, A., & Haridy, S. (2021). Requirements, challenges and impacts of Lean Six Sigma applications – a narrative synthesis of qualitative research. *International Journal of Lean Six Sigma, 12*(2), 318-367. https://doi.org/10.1108/IJLSS-06-2019-0067

Aljuraid, R., & Justinia, T. (2022). Classification of Challenges and Threats in Healthcare Cybersecurity: A Systematic Review. Studies in Health Technology and Informatics, 295, 362-365. https://doi.org/10.3233/shti220739

Alvarenga, A., & Tanev, G. (2017). A Cybersecurity Risk Assessment Framework that Integrates Value-Sensitive Design. *Technology Innovation Management Review, 7*(4), 32-43. http://ezproxy.jamk.fi:2048/login?url=https://www.proquest.com/scholarly-journals/cybersecurity-risk-assessment-framework-that/docview/1963139581/se-2

Asosheh, A., Hajinazari, P., & Khodkari, H. (2013). A practical implementation of ISMS. https://doi.org/10.1109/ECDC.2013.6556730

Bashofi, I., & Salman, M. (2022). Cybersecurity maturity assessment design using NISTCSF, CIS CONTROLS v8 and ISO/IEC 27002. In 2022 IEEE International Conference on Cybernetics and Computational Intelligence (CyberneticsCom) (pp. 58-62). Malang, Indonesia, IEEE. https://doi.org/10.1109/CyberneticsCom55287.2022.9865640

Bhuyan, S. S., Kabir, U. Y., Escareno, J. M., Kenya, E., Sandeep, P., Wyant, D., Sajeesh, K., Levy, M., Satish, K., Dipankar, D., & Aram, D. (2020). Transforming Healthcare Cybersecurity from Reactive to Proactive: Current Status and Future Recommendations. *Journal of Medical Systems, 44*(5) https://doi.org/10.1007/s10916-019-1507-y

Brody, R. G., Chang, H. U., & Schoenberg, E. S. (2018). Malware at its worst: death and destruction. *International Journal of Accounting and Information Management, 26*(4), 527-540. https://doi.org/10.1108/IJAIM-04-2018-0046

Cawthra, J., Ekstrom, M., Lusty, L., Sexton, J., Sweetnam, J., & Townsend, A. (2020, December). Data integrity: Detecting and Responding to Ransomware and Other Destructive Events. Executive Summary - NIST SP 1800-26 documentation. Retrieved April 14, 2024, from https://www.nccoe.nist.gov/publication/1800-26/VolA/index.html

Continuous Improvement Model - continual improvement tools | ASQ. (n.d.-a). Retrieved April 9, 2024, from https://asq.org/quality-resources/continuous-improvement

ENISA. (2022, November 8). Need. Retrieved April 9, 2024, from https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-isms/need

Embracing the unknown by constructing an organizational cybersecurity strategy: The knowledge-led art of balancing risk against the cost of protection. (2020). *Strategic Direction, 36*(2), 24-26. https://doi.org/10.1108/SD-10-2019-0213

European Union Agency for Network and Information Security. (2018, January). *Reference incident classification taxonomy*. https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy

Farahbod, K., Shayo, C., & Varzandeh, J. (2022). SIX SIGMA AND LEAN OPERATIONS IN CYBERSECURITY MANAGEMENT. *Journal of Business and Behavioral Sciences, 34*(1), 99-109. http://ezproxy.jamk.fi:2048/login?url=https://www.proquest.com/scholarly-journals/six-sigma-lean-operations-cybersecurity/docview/2667274873/se-2

Ghadge, A., Weiß, M., Caldwell, N. D., & Wilding, R. (2020). Managing cyber risk in supply chains: a review and research agenda. Supply Chain Management, 25(2), 223-240. https://doi.org/10.1108/SCM-10-2018-0357

Harry, M. J., Mann, P. S., De, H. O. C., Hulbert, R. L., & Lacke, C. J. (2010). Practitioner's guide to statistics and lean six sigma for process improvements. John Wiley & Sons, Incorporated.

IBM. (2024, April 2). What are security controls? Retrieved April 9, 2024, from https://www.ibm.com/topics/security-controls

Investing in cybersecurity: Gaining a competitive advantage through cybersecurity. (2021). *Strategic Direction, 37*(2), 19-21. https://doi.org/10.1108/SD-11-2020-0205

Kari Lukka. (2003, January). The Constructive Research Approach. ResearchGate. https://www.researchgate.net/publication/247817908_The_Constructive_Research_Approach

Kattavat Palvelut Kuluttajille ja ammattilaisille. Fimlab. (2020-a). Retrieved October 7, 2022, from https://fimlab.fi/palvelut#kuluttajalle

Kattavat Palvelut Kuluttajille ja ammattilaisille. Fimlab. (2020-b, April 8). Retrieved October 7, 2022, from https://fimlab.fi/palvelut#ammattilaiselle

Koskinen, S., (2023). Kyberturvallisuuden toteutuminen alihankintaketjuissa, https://urn.fi/URN:NBN:fi:amk-2023082925062

What is lean?: Lean thinking. Lean Enterprise Institute. (2023, January 27). Retrieved May 15, 2024, from https://www.lean.org/explore-lean/what-is-lean/

Liesoja, J., (2023). Cyber security risk management method for hospital pharmacy: pharmaceutical service operations, https://urn.fi/URN:NBN:fi:amk-2023090525353

Literature review. The University of Edinburgh. (2024, February 26). Retrieved May 15, 2024, from https://institute-academic-development.ed.ac.uk/study-hub/learning-resources/literature-review

Loi, M., Christen, M., Kleine, N., & Weber, K. (2019). Cybersecurity in health – disentangling value tensions. *Journal of Information, Communication & Ethics in Society, 17*(2), 229-245. https://doi.org/10.1108/JICES-12-2018-0095

Mahmoodi, E., Fathi, M., & Ghobakhloo, M. (2022). The impact of Industry 4.0 on bottleneck analysis in production and manufacturing: Current trends and future perspectives. Computers & Industrial Engineering, 174, 108801. https://doi.org/10.1016/j.cie.2022.108801

Malatji, M., Sune, V. S., & Marnewick, A. (2019). Socio-technical systems cybersecurity framework. *Information and Computer Security, 27*(2), 233-272. https://doi.org/10.1108/ICS-03-2018-0031

Monipuoliset Laboratoriopalvelut Jokaisen Arkeen. Fimlab. (2022, March 16). Retrieved October 7, 2022, from https://fimlab.fi/

National Institute of Standards and Technology. (2014). Framework for improving critical infrastructure cybersecurity. U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.04162018

National Supervisory Authority for Welfare and Health. (n.d.). *Information systems for social welfare and healthcare*. Valvira. https://valvira.fi/en/information-systems-for-social-welfare-and-healthcare

Nicho, M. (2018). A process model for implementing information systems security governance. *Information and Computer Security, 26*(1), 10-38. https://doi.org/10.1108/ICS-07-2016-0061

Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017). An introduction to information security. An Introduction to Information Security, 1(1). https://doi.org/10.6028/nist.sp.800-12r1

Nishani, E. V., & Pinsker, R. (2020). IT risk management: interrelationships based on strategy implementation. *International Journal of Accounting and Information Management, 28*(3), 553-575. https://doi.org/10.1108/IJAIM-08-2019-0093

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., et al. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ, 372, n71. https://doi.org/10.1136/bmj.n71

Piercy, N., & Rich, N. (2015). The relationship between lean operations and sustainable operations. *International Journal of Operations & Production Management, 35*(2), 282-315. https://doi.org/10.1108/IJOPM-03-2014-0143

Poth, A., Kottke, M., Middelhauve, K., Mahr, T., & Riel, A. (2021). Lean integration of IT security and data privacy governance aspects into product development in agile organizations. *J. Univers. Comput. Sci.*, *27*(8), 868-893

Pousi, K., (2022). Kuntien kyberturvallisuushaasteet ja niihin varautuminen, https://urn.fi/URN:NBN:fi:amk-2022092220366

Prisma 2020 statement. PRISMA statement. (n.d.-a). https://www.prisma-statement.org/prisma-2020-statement

Suni, E., (2021). Kyberhäiriöiden hallinnan prosessien ja toimintaohjeiden kehittäminen terveydenhuollon ympäristöissä, https://urn.fi/URN:NBN:fi:amk-202102192485

Taghavifard, M. T., Dadvand, A., & Aghaei, M. (2018). Improving Service Processes and Reducing Waiting Times for Bank Customers Using Simulation Approach. *Business Intelligence Management Studies*, *6*(22), 75-105. doi: https://doi.org/10.22054/ims.2018.8521

WHO. (n.d.). The protection of personal data in Health Information Systems. The protection of personal data in health information systems – principles and processes for public health. Retrieved April 15, 2024, from https://iris.who.int/bitstream/handle/10665/341374/WHO-EURO-2021-1994-41749-57154-eng.pdf

Wolniak, R., Skotnicka-Zasadzień, B., & Gębalska-Kwiecień, A. (2018). Identification of bottlenecks and analysis of the state before applying lean management. EDP Sciences. https://doi.org/10.1051/matecconf/201818301001

Yritys. Fimlab. (2023, March 14). Retrieved May 9, 2022, from https://fimlab.fi/yritys

Appendices

Appendix 1. PRISMA_2020_abstract_checklist

Section and Topic	Item #	Checklist item	Reported (Yes/No)
TITLE			
Title	1	Identify the report as a systematic review.	
BACKGROUND			
Objectives	2	Provide an explicit statement of the main objective(s) or question(s) the review addresses.	
METHODS			
Eligibility criteria	3	Specify the inclusion and exclusion criteria for the review.	
Information sources	4	Specify the information sources (e.g. databases, registers) used to identify studies and the date when each was last searched.	
Risk of bias	5	Specify the methods used to assess risk of bias in the included studies.	
Synthesis of results	6	Specify the methods used to present and synthesise results.	
RESULTS			
Included studies	7	Give the total number of included studies and participants and summarise relevant characteristics of studies.	
Synthesis of results	8	Present results for main outcomes, preferably indicating the number of included studies and participants for each. If meta-analysis was done, report the summary estimate and confidence/credible interval. If comparing groups, indicate the direction of the effect (i.e. which group is favoured).	
DISCUSSION			
Limitations of evidence	9	Provide a brief summary of the limitations of the evidence included in the review (e.g. study risk of bias, inconsistency and imprecision).	
Interpretation	10	Provide a general interpretation of the results and important implications.	
OTHER			
Funding	11	Specify the primary source of funding for the review.	
Registration	12	Provide the register name and registration number.	