Cyber security risk management method for hospital pharmacy

Pharmaceutical service operations

Jari Liesoja

Master's thesis
Aug 2023
Master's Degree Programme in Information Technology, Cyber Security

Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Jari Liesoja

Cyber security risk management method for hospital pharmacy, Pharmaceutical service operations

Jyväskylä: Jamk University of Applied Sciences, August 2023, 75

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

Permission for open access publication: Yes

Language of publication: English

Abstract

Social- and healthcare sector has undergone major changes in Finland due to reorganizing of social-, healthcare- and rescue services and new wellbeing service counties have started their operation in 2023. Modern technological solutions have been adopted and the role of digitalized services is increasing, and that change has also affected cyber security threats and risks. The purpose of this research was to recognize cyber security risks evolving from pharmaceutical services digital operations in hospital pharmacy and develop a method for controlling those. Research was conducted using a design research approach with qualitative methods. Data was retrieved using professional literature and documentation, questionnaire, workshops, and interviews and based on the acquired information, the model of the method was designed. The study managed to produce a distinct model for controlling cyber security risks evolving from the pharmaceutical services’ digital operations in hospital pharmacy environment. The developed method connects case organization’s internal policies, currently existing legal requirements for cyber security risk management, business need for improving cyber security risk procedures and the goal to produce principles to pharmacy personnel, how to recognize cyber security threats and risks in their normal daily operations.

Keywords/tags (subjects)

Cyber security, risk management, healthcare, pharmaceutical service, information security

Miscellaneous (Confidential information)

-

Contents

Figures

Tables

1 Introduction

Recognizing and understanding the vulnerabilities, threats and risks in your business is crucial in today's all time changing environment to be able to deliver continuous business operations. In this way we manage to design and evaluate needed countermeasures or safeguards against unwanted situations and increase our resilience. Lehto et al. (2019) mentions in their study covering cyber security in social and healthcare, that cyber-attacks can influence organizations at a strategic level if the target of the attack is to damage the whole business. As businesses develop to meet current requirements and adopt new possibilities to meet those, we can see our operational environment to change into direction, which is not instantly visible to us and include major risks due to cyber dimension (Boyens et al., 2021).

Healthcare sector is a remarkably interesting target to malicious attackers primarily because of the data it has. This data includes both patients' personal information and health information and is estimated to be the most valuable information in today's market (Coventry & Branley, 2018). This type of data must be kept safe according to the European Union law "The General Data Protection Regulation (GDPR)", which directs how this type of data may be processed and handled in all its forms. Lehto et al. (2019) states, that organizations do not recognize attacks or data thefts on time, and this might cause investigation problems. This observation corresponds with PricewaterhouseCoopers' report on cyber-attack against The Health Service Executive (HSE) in Ireland, where the attacked implemented injection on Mach 18th 2021 and attack was recognized on 14th of May 2021. During this time, the attacker had a possibility to perform malicious activities in HSE environment and recovery to normal state can be problematic and take long time (Conti Cyber Attack on the HSE, 2021).

When discussing healthcare and personal information, we are obligated to follow the national laws and rules when handling that information. The problem here is not that we would not have enough regulation in place but rather understanding how we can implement sufficient countermeasures to protect the data, network, identities, mobile phones, tablets, workstations, laptops, or servers. For this, we must consider our business, field of operations, and try to recognize those threats, vulnerabilities and risks we might have in our operations. Muthuppalaniappan and Stevenson (2021) highlight in their article healthcare sector to be responsible to organize cyber security risk management to meet the threats evolving from cyber-space.

This study focuses on recognizing cyber security risks originating from the pharmaceutical services including supply chain structures in hospital pharmacy operations and implementing method to case organization, how to recognize and control cyber security risks as part of their daily function. Protecting pharmaceutical services is important to protect the patient's health and service continuity in social and healthcare. We must recognize those parts of the pharmaceutical services supply chain, which are vulnerable to cyber security threats and includes information technology. With this approach we can identify cyber security risks compromising the services, which might not be recognized yet in the operations. This information is needed to design a process and model of cyber security risk management for hospital pharmacy to support their daily operations. The management model must cover the important parts of the supply chain digital services and information technology solutions adopted.

This study does not cover the whole information technology environment in any social- or healthcare sector operations. This is a limited view to pharmaceutical services in hospital pharmacy operations. Accordingly, this study does not include all the different third parties which can be used to deliver services and it is limited to case organization only.

The abstract section will indicate the essential findings and conclusions of the study. In the first (1) chapter is the introduction to this thesis study and express the topic, research questions and the target and goal of the research. The second (2) chapter describes the research approach and methods used for data acquisition. Theory and literature review is discussed in chapters three (3), four (4) and five (5) and these introduces digitalization in healthcare, structures of pharmaceutical supply chain in Finland and cyber security risk management procedures to consider. Chapter six (6) describes collected data from the documentation, questionnaire, workshops, and interviews. Designing of the cyber security risk management model including method, checklists, process, and monitoring criteria are presented in chapter seven (7). Results and findings in chapter eight (8) collect the existing data with the pursued target of the research and describe the validity and relevancy, reliability, and ethicality of the study. Conclusions are addressed in chapter nine (9) and discussion in chapter 10 is the closing chapter of this research.

1.1 Research topic

The topic of the research is to discuss pharmaceutical service operations in hospital pharmacy and how cyber security risks evolving from digitalized services in pharmaceutical service supply chain should be recognized and controlled. Digitalization has a significant role in current pharmaceutical services and risks are changing along with digitalization and new services. Pharmaceutical services supply chain overall is designed to deliver lawful medicines to its clients (Brechtelsbauer et al., 2016). Integrating new technology with pharmaceutical supply chain transforms the risk matrix of the traditional supply chain structure and cyber security risks must be considered for integrity, availability, and continuity of the services (Boyens et al., 2021).

The Ministry of Finance mentions on its web pages, that Finland is under huge reform, which includes digitalization. This digitalization is also covering new services for the starting welfare counties and is one aspect of the research. How might this affect the risk factors in cyber security concerning hospital pharmacy operations? (The Ministry of Finance, Digitalization).

The scope of this study is to examine pharmaceutical service operations in hospital pharmacy and develop a method for controlling cyber security risks evolving from pharmaceutical service operations. Case organization is one of the 21 wellbeing services counties in Finland producing social-, healthcare-, and rescue services to the citizens (The Ministry of Finance, duties and other activities). Hospital pharmacy and pharmaceutical services are critical functions of the central hospital regarding patient safety and care, and furthermore serve comprehensively wellbeing services county operations. Pharmacy operations concern over 10 000 employees and around 300 000 citizens, who will be clients to the wellbeing services county.

Risk management is a continuous process in case organization and management duties are divided into various levels in the organization. The reason for risk management is to coordinate activities to control risks (ISO/IEC 31000:2018, 2018). Pharmacy operations are increasingly using information technology and new threats and risks emerge along with modern technology and changes in operations. Cyber security risk management needs to be developed to meet organization’s responsibilities and requirements in this changing environment to improve the organization ability to be prepared against abnormal situations.

1.2 Research questions

According to the topic of the study discussed in the previous chapter, research questions are set to correspond existing research problem. The problem is that case organization has a need to improve cyber security risk management to correspond with altered pharmaceutical service operations in hospital pharmacy. To meet the requirement of improving cyber security risk management, the following questions are composed for this research. The main question emphasizes the problem with the methods to use to recognize and manage cyber security risks within pharmaceutical services. Correspondingly secondary supporting questions focuses to analyze prospects for developing applicable cyber security risk management process and to understand the capabilities and the aspiration of the personnel working for the hospital pharmacy in case organization.

Main research question:

1. What kind of method could be used to recognize and manage cyber security risks emerging from the pharmaceutical services supply chain in hospital pharmacy operations?

Secondary research questions to support this work:

1. How can we achieve a consistent cyber risk management model for hospital pharmacy promoting risk management and cyber security management frameworks and standards?
2. How do the hospital pharmacy personnel understand and experience cyber security risks in their daily operations?

1.3 Target and goal of the research

Pharmaceutical services in hospital pharmacy and hospital operations are crucial functions for patient care and safety. This service must be protected from internal and external threats covering the whole existing operation chain. This study approaches pharmaceutical services in hospital pharmacy operation and does not cover patient care. The target within this study is to express the threats originating from the pharmaceutical service digital structures in pharmacy operation and the goal is to produce principles to pharmacy personnel, how to recognize threats and risks in their normal daily operations delivering pharmaceutical services to whole wellbeing service county and to other agreement-based clients.

To rationalize this study, we must consider the main function of the pharmaceutical service operations in hospital environment to deliver continuous and on-time pharmaceutical service for its clients. In this context, we need to understand the employees' abilities in cyber security risk management as well as the operational environment these healthcare professionals are working in. These professionals are not always familiar with cyber security and information technology, but are involved in purchasing, arranging, and controlling the whole supply chain regarding the pharmaceutical service operation considering hospital pharmacy. They need to have policies, procedures, and guidance in place for responsibilities, directions, arrangements and communications of cyber security threats and risks management as part of their normal business. Underestimating this might expose the organization to unknown risks and compromise security and continuity.

With this study, the case organization can develop its abilities to control cyber security risks in its service operation. Results of this study can be utilized with another risk management processes and with other welfare regions in Finland with similar services.

2 Research approach and methods

2.1 Research approach

This research is based on the actual development need for cyber security risk management on pharmaceutical service operations in hospital pharmacy. Current model of cyber security risk management must be developed according to the business and the constantly evolving threat matrix. It was identified that there is a gap between cyber operations and the pharmaceutical service supply chain digital operations, and this thesis work is targeted to revise missing elements of cyber security management in case organization for this. The challenge is that case organization could not recognize the lacking elements, and this must be studied before remodeling the cyber security risk management procedures to allocate the countermeasures competently.

This study is targeted to achieve change in cyber security procedures as part of complete cyber security management. Understanding of the phenomenon and operational environment is particularly important in this study, which could direct this study close to case research (Kananen, 2013, 29). From another point of view, this study involves some intervention of researcher and with the set target of change in cyber security procedures, the approach could be action research. According to Kananen (2013, 24), the change is a key factor in design research approach. The difference between action study and design research is the researcher's role, as in the action research approach, the researcher is more actively involved with the development and intervention (Kananen, 2013, 29).

As the methods of this study are qualitative and the result of the study aims to improve the existing procedures of cyber security risk management with the limited amount of intervention by the researcher, the research approach is chosen to be design research with qualitative methods.

The structure of this research is divided into various sections (Figure 1). According to Kananen (2013, 23), the process of design research encompasses the original status of the research subject and the aimed target with the measurable changes implicated by the research. Section one includes status analysis, section two covers data collection and analysis. Section three is to develop a new risk management model according to the set target. Section four introduces developed model to the business and last section five is for conclusion.

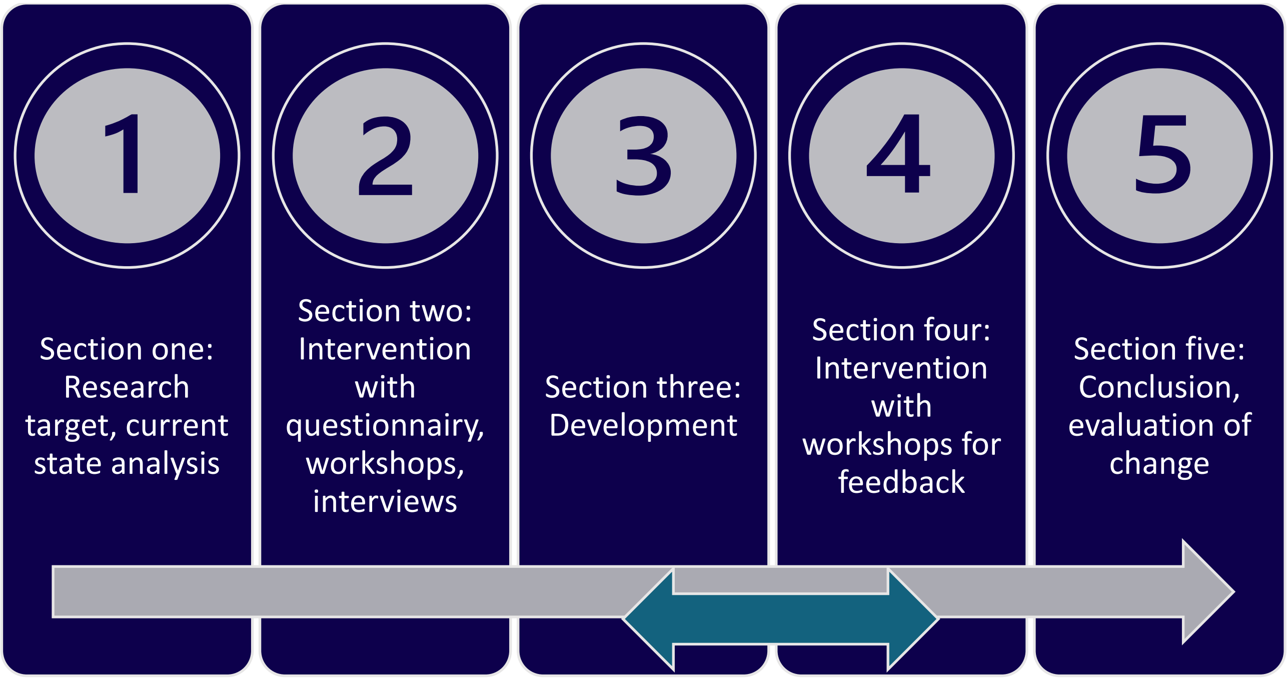
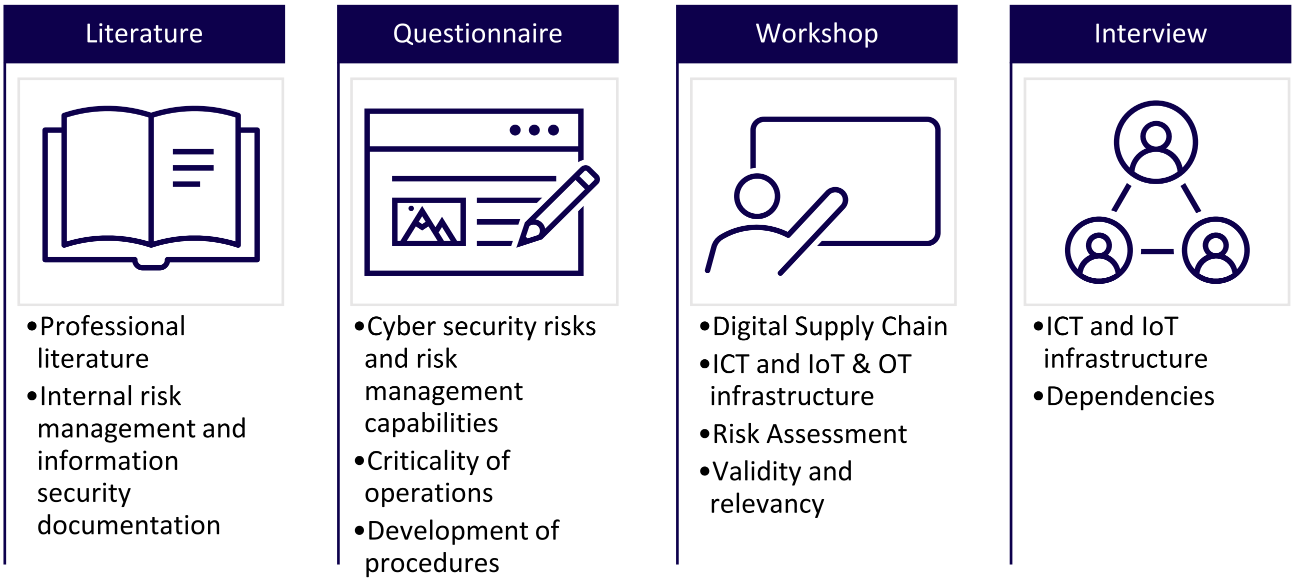

1
2
3
4
5
Section one: Research target, current state analysis
Section two: Intervention with questionnairy, workshops, interviews
Section three: Development
Section four: Intervention with workshops for feedback
Section five: Conclusion, evaluation of change

Figure 1, Research process

2.2 Data acquisition methods

Data used in this study is collected using multiple methods. Information discussing cyber security and risk management is achieved using articles, standards, frameworks, professional literature, and publications. Because this study is limited to pharmaceutical services operation in hospital pharmacy environment, questionnaire, workshops and interviews to pharmacy personnel and ICT-personnel of the case organization is being used as data collection methods among with literature (Figure 2, Data Acquisition Methods).



Literature

- Professional literature
- Internal risk management and information security documentation

Questionnaire

- Cyber security risks and risk management capabilities
- Criticality of operations
- Development of procedures

Workshop

- Digital Supply Chain
- ICT and IoT & OT infrastructure
- Risk Assessment
- Validity and relevancy

Interview

- ICT and IoT infrastructure
- Dependencies

Figure 2, Data Acquisition Methods

2.2.1 Literature and documentation

2.2.1.1 Literature

Professional literature, journals, and articles regarding cyber security in healthcare were searched using several sources and time period between 2013 and 2023. The main sources were Google Scholar, Janet.finna.fi, https://link.springer.com/, https://www.nist.gov/ for cyber security in healthcare related information and Google Search Engine for dedicated web pages including additional information.

Key phrases for searches:

- “Adopting standards and frameworks for information security”
- “Cyber security culture in healthcare”
- “Cyber security in healthcare”
- “Cyber security management in healthcare”
- “Cyber security risk management in healthcare”

- “Cyber security risk management pharmaceutical service”
- “Cyber security risks in pharmaceutical supply chain”
- “Cyber security risk management system”
- “Cyber security threats in healthcare”
- “Cyber security trends in healthcare”
- “Framework for improving critical infrastructure cybersecurity”

Articles, journals of books which were not free, or access was not available with JAMK student credentials, or the given credentials of case organization, were not used in the study.

2.2.1.2 Documentation

Case organization has implemented comprehensive internal administrative level documentation concerning risk management, information and cyber security management and data privacy management to use internally. These documents include

- Administrative Regulations including risk management responsibilities
- Information Security and Data Privacy Policy
- Information Security and Data Privacy Procedures
- Information and Cyber security Architecture principles.

These documents are used in this study as guidance to risk and cyber security management in case organization.

Case organization uses intranet service as information sharing and communication channel to its employees. The intranet service comprises separate information security and data privacy pages and is available to all employees working for the organization. Information security and data privacy pages encompass training courses for the employees to execute in diverse positions of case organization. Performing these courses is followed by the superiors.

2.2.2 Questionnaire

The link to the questionnaire is delivered to participants via email sent by the dedicated pharmacy employee. The questionnaire is divided into two (2) chapters and aligned with the secondary research question, “How do the hospital pharmacy personnel understand and experience cyber security risks in their daily operations?”

The first chapter includes six (6) questions with open answer possibilities. It is used to collect information how hospital pharmacy personnel understand cyber security risks and risk management, how they experience their possibilities and capabilities to recognize cyber security risks and how cyber-attacks against pharmaceutical service supply chain could influence organizations performance.

The second chapter combines three (3) separate questions with closed multiple answer options. The first question is to get information, how the participant experience presented numerous answer choices to be connected to cyber security risk management of pharmaceutical services. The first question has 13 separate alternatives, and the participant can choose as many as he/she can identify. The second question specifies the need of improving cyber security risk management in case organization and indicates how participants understand cyber security risks management. This question has nine (9) answer choices, and the participant can choose as many he/she can identify. The last question indicates the need to improve information and cyber security procedures in the case organization and presents eight (8) separate claims of which the participant can choose as many as he/she can identify.

2.2.3 Workshops

Research includes five (5) workshops, of which three (3) processes the pharmaceutical supply chain for hospital pharmacy, digital services in supply chain regarding pharmaceutical services in hospital pharmacy, ICT, IoT (Internet Of things) and OT (Operational Technology) infrastructure in hospital pharmacy and cyber security risks evolving from these aspects. Based on results and findings from these three workshops, questionnaire, and interviews, the fourth (4) and fifth (5) workshops address the proposal for the risk management process and method. The proposal will be evaluated by the ICT personnel in workshop four (4) and by the pharmacy and ICT personnel in workshop five (5) for validity and relevancy.

2.2.4 Interviews

Interviews, both group and one-to-one, are to specify used information technology solutions and dependencies to other hospital services and service providers, which could influence to hospital pharmacy operations and should be considered as dependencies to business continuity either explicitly or indirectly. In this research, three (3) to five (5) interviews are needed to discourse the information gathered from the workshops.

3 Digitalization in healthcare

Digitalization in Finland by the Ministry of Finance is challenging Finnish society to organize and develop public services in a way, which will influence public healthcare services, and the way these services are used in the future (The Ministry of Finance). This transformation requires leadership to ensure citizens confidentiality into public healthcare services as well as government to response with concurrent regulatory in changing environment. According to Bhuyan et al. (2020), regulatory must be aligned with a larger view containing cyber security issues in our society to ensure, that new innovations and modern technology solutions can be used legally in healthcare to protect the sensitive data and the patients. New digitalized services require built-in security and privacy approach as no recent technology itself cannot solve this problem with cyber security challenges within digitalization. Digitalization of the new medical services for the citizens requires a strong cyber security approach in service planning. Information and cyber security can be considered as an enabler when planning new digital services.

In this transformation process, it is mandatory to take care of personal rights and lawfulness while processing personal data within digital services. Data Protection Act (2018/1050) directs both the lawfulness processing situations and how personal data must be protected while processing or storing this type of data. In public health care, the processing of substantial amounts of personal data is typical and consists of information about a person’s health. This type of special category data must be protected using both administrative and technical security measures to minimize risks caused by the operations of handling health information of the registered citizen (Data Protection Act 1050/2018).

Nifakos et al., (2021) announce in their systematic review, that vulnerabilities in systems as well as deficiencies among humans are obstacles considering digital transformation and digitalization. The change in ways of using patient information also alters the cyber security risk management procedures. According to their review, healthcare sector is behind with their cyber security procedures compared to other industries in protecting their services and patient information despite healthcare organizations have implemented cyber security policies and procedures to be able to protects their clinical services. They highlight the importance of healthcare personnel cooperation in successful cyber security risk management and expresses the need for cyber security training and information of cyber security threats in healthcare and digital services (Nifakos et al., 2021).

4 Pharmaceutical supply chain structure in Finland

The Finnish Medicines Agency Fimea supervises, develops, and regulates pharmaceuticals (medicinal, medical devices, blood and tissue products and biobanks) in Finland. This encompasses the pharmaceutical services in hospitals combining medicine manufacturing and hospital pharmacy operations (Fimea, 2023).

According to fimea.fi web pages, Fimea focuses on pharmaceutical operation acting as an authority to pharmaceutical service providers. The main task is to develop and maintain the population health in Finland. Fimea directs pharmacies operating in hospitals in Finland and regulates the manufacturing of medicines in hospital pharmacies. Fimea endorses pharmaceutical wholesale dealers in Finland and monitors the mandatory stockpiling obligation by the Act on Compulsory Stockpiling of Medicinal Products (979/2008), which comprise healthcare service units, medicinal product manufacturers, medical product importers and the Finnish Institute of health and welfare (Fimea, 2023, pharmaceutical industry).

As an authority, Fimea controls the safety and regulation of medical devices by setting mandatory specifications for medical device manufacturing and their use. The European Union controls medical devices in larger scale and has implemented EU regulations for medical devices 2021 (Fimea, 2023, medical devices).

4.1 Distribution of pharmaceuticals

Pharma Industry Finland (PIF) announces, that distribution of medicines is very firmly controlled process using one-channel assumption for acquiring of the medicines. The process requires pharmacies or hospital pharmacies to use designated wholesale supplier for each medicine. Process aims both to protect the users of the medicines by preventing fraudulent medicines and securing the availability of the medicines (Pharma Industry Finland, n.d., distribution of pharmaceuticals).

The supply chain structure starting from the medicinal ingredients ending to the user of the medicine is long. It might take up to two (2) years before the medicine is ready for distribution from the factory. Hospital pharmacies are in the back end of the whole supply chain structure (Figure 3) still having a significant role in the supply chain considering pharmaceutical service operations (Lääketeollisuus, n.d., lääkkeiden jakelu).

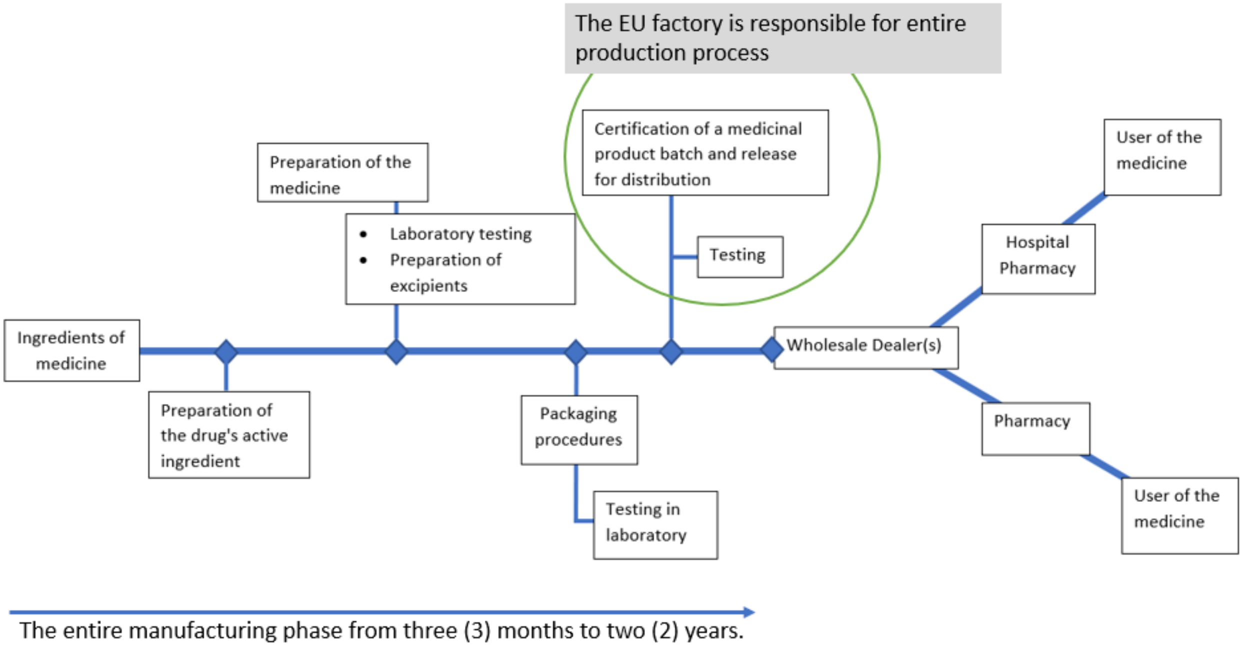

The EU factory is responsible for entire production process
Certification of a medicinal product batch and release for distribution
Testing
Preparation of the medicine
Laboratory testing
Preparation of excipients
Ingredients of medicine
Preparation of the drug's active ingredient
Packaging procedures
Testing in laboratory
Wholesale Dealer(s)
Hospital Pharmacy
User of the medicine
Pharmacy
User of the medicine
The entire manufacturing phase from three (3) months to two (2) years.

Figure 3, Pharmaceutical supply chain structure (based on Lääketeollisuus, n.d., lääkkeiden jakelu)

4.2 Finnish Medicines Verification, FiMVO

As part of the pharmaceutical supply chain structure, pharmacies have a key role in preventing fraudulent medicines getting to the patients. Pharmacies, including hospital pharmacies, use the verification system for each medicine to check its validity before distributing it further on because fraudulent medicines are highly unlikely to be identified otherwise. The verification system is being used from 2019 and it is controlled by FiMVO. The verification system covers the whole pharmaceutical supply chain from the manufacturer to the pharmacy (Pharma Industry Finland, n.d., medicines verification system).

4.3 Hospital pharmacies

According to the Fimea (2023), there are 25 hospital pharmacies in Finland. These pharmacies provide a large variety of pharmaceutical services to their customers and can also produce medicines themselves directed by Fimea regulation 6/2011 (Apteekkien lääkevalmistus), European Union guidelines and principals, “Guide to Good Manufacturing Practice for Medical Products”, Fimea regulation 5/2012 (Lääkkeiden hyvät tuotantotavat) and regulation 6/2012 (Sairaala-Apteekin ja lääkekeskuksen toiminta). Hospital pharmacies are a critical function of the main hospital services producing pharmaceutical services inside the hospital which delivers medical services to citizens directed by the Health Care Act (1326/2010). Like pharmaceutical services, cyber security threats can also affect patient health. The number of cyberattacks in healthcare is increasing, and this will affect service providers to organize comprehensive risk management into new ways including cyber security risks management.

5 Cyber security risk management

5.1 Strategic approach to risk management

The reason for risk management is to coordinate activities to control existing risks (ISO/IEC 31000:2018, 2018). Organizations are different, and their businesses differ from one another. Management decisions to protect businesses and willingness to tolerate risks are affecting their cybersecurity control implementations. Because cyber security control implementation depends on the business' own target within larger business risk management, the management needs to align the cybersecurity controls and goals with the business targets (Taherdoost, 2022).

According to Finnish Cyber Security Strategy and Implementation (Sillanpää, Roivainen & Lehto, 2015), a strategy usually focuses on making change in the organization. With the defined strategy, the organization moves from the current situation towards the new situation, which management has determined to be the goal of the change. For this, they present, that first we need to understand our current environment and all the elements in it. Based on current state analysis results, we can identify the weaknesses and strengths we have in our environment and have a solid base to create our strategy.

Information and cyber security strategy should reflect and support organizations primary strategy. Information and cyber security have been notified to be one key area on healthcare service production to maintain resiliency and continuous service production. Act on Information Management in Public Administration (906/2019) also impacts information security implementation in health care. This law promotes understanding of existing risks and controlling of change management in organizations environment. Organization should understand the possible impact in its operations when the planned change could affect to information management, operations, or interoperability between public authorities (Act on Information Management in Public Administration, 906/2019).

5.2 Approach to cyber security risk management in healthcare

European Union Agency for Network and Information Security (ENISA) published a report of smart hospitals in 2016; *"Smart Hospitals: Security and Resilience for Smart Health Service and Infrastructures".* In this research, term "smart hospital" is defined in to following way: *"A smart hospital is a hospital that relies on optimized and automated processes built on an ICT environment of interconnected assets, particularly based on Internet of things (IoT), to improve existing patient care procedures and introduce new capabilities"* (European Union Agency for Cybersecurity, 2016).

According to the ENISA Smart Hospital report, although threats typical to smart hospitals are connected to the information technology solutions and systems facilitating the smart hospital environment, we must not forget the human factor causing system failures or errors handling data instead of focusing purely on malicious activities. They emphasize the fact that understanding your own environment and the risks in it is particularly important to be able to implement correct security functions in place. ENISA study recommends, that hospitals should at least

- implement risk assessment
- create information sharing channels between hospitals
- implement technical penetration testing and auditing for verifying and managing the vulnerabilities
- participate and emphasize Information Sharing and Analysis Centre (ISAC) group work (European Union Agency for Cybersecurity, 2016).

Digital Pool, coordinated by Finnish National Emergency Supply Agency, conducted a study in 2020 concerning cyber security current state in different industries including healthcare, and covered 12 industries with over 100 organizations (Digital Pool, 2020a). The study indicates differences between industries but also underlines that digitalization is mandatory for businesses and cyber security must be aligned with business requirements. Management support and engagement is needed to create a successful cyber security program in the organization. This study expresses the importance of management commitment to cyber security to have continuity and relevancy with the development program instead of developing cyber security based on individual expert's skills and motivation (Digital Pool, 2020b.).

The result of the Digital Pool study shows that there is remarkable variance between the industries and healthcare sector must consider data privacy among with cyber security. They present, that cyber security personnel must be trained more, and situation awareness must be developed. (Digital Pool, 2020b.) To the extent of training cyber security personnel, Gioulekas et al. (2022) states in their article the criticality of the healthcare systems and expresses the importance of healthcare information and end user training as part of cyber security.

Similar observations can be found from other studies including different viewpoints. End users, the insiders, have a key role establishing cyber security in healthcare. These end users have both physical access to the premises and access to the systems. Adebukola et al. (2022) illustrates insider threats in healthcare sector as one cyber security threat to be recognized. According to their research this does not mean insiders being purposeful in making cyber-attacks rather than not understanding or making a mistake. Weak passwords, human errors, and ignorance of existing legislation in healthcare are serious threats in cyber security, which can be associated both with ENISA and Digital Pool studies earlier in this chapter. Bhuyan et al. (2020) presents in their research that end users including both former and current employees have been arranging 48% of the data breaches and only 10% were not deliberately done. This expresses and supports the importance of the cyber security awareness program and training implementations in the organization, which was Digital Pool (2020b) recommendation.

According to Bhuyan et al. (2020) cyber security breaches in systems are consequences of the mistakes made by the developers. These mistakes endanger the systems used by the end users under cyber-attacks and might lead to serious cyber security deflections and data breaches. These types of vulnerabilities are an extensive dilemma when acquiring new systems and solutions for the business. Adebukola et al. (2022) states that around 90% of security events concern vulnerabilities in software level. To control this type of vulnerabilities in public healthcare, like described in chapter three, Data Protection Act (2018/1050) and Act on Information Management in Public Administration (906/2019) 15 § - 17 § steers organizations to control risks within data and systems.

The National Cyber Security Centre Finland (NCSC-FI) published the requirements for information security and data protection in social and healthcare developed as one part of the Kyber-Terveys project 2018-2019 advocated by the National Emergency Supply Agency. These requirements can be used when planning the procurement of the new system and as requirements for the system and suppliers for controlling risks (The National Cyber Security Centre, 2022).

Complexity of the information technology infrastructure, the considerable number of applications combined with the enormous number of the employees in healthcare and the sensitivity of the data, creates the cyber security risk matrix for the healthcare organization. Information technology systems are evolving constantly along with the needs of medical care. There are always things to be considered like access to the patient information in case of urgent treatment and access to the systems. We must not endanger the patient care with cyber security implementations and risks should be recognized and assessed before decisions. Cyber security risks management is one area to be considered and established in healthcare organizations (Bhuyan et al., 2020).

The information technology environment and various applications need to be controlled and managed effectively. Information security should not be separated from other information technology as the base for information security is built upon professionally managed and reliable information technology infrastructure (Argaw et al., 2020). Coventry and Branley (2018) highlight correspondingly information technology to be concern for information security because of increment in connected devices, growth in mobile devices in healthcare and using health devices outside of hospital environment. As discussed in chapter three (3), Digitalization in Healthcare, cyber security should be considered when planning the digitalization of services to ensure resilience and continuity of the services.

Should cyber security risk management procedures focus purely either on technology vulnerabilities or human factors? As discussed earlier, focusing only on certain areas of organization’s capabilities and threats does not result in a consistent approach to cyber security risk management. According to the Nifakos et al. (2021) systematic review, substantial amount of information security breaches are caused by employees who have not adopted organizational policies or legislation. Concentrating purely on solving challenges evolving from the technology does not change this behavior and because of this founding, cyber security risk management should not focus only on analyzing threats, vulnerabilities, and consequences on technology solutions. Human factors and employees’ abilities to face information security factors should be considered as well (Nifakos et al., 2021).

5.2.1 Trends of the cyber-attacks in healthcare

As discussed in the previous chapter, the complexity of information technology and information systems in healthcare increases cyber security risks. Wireless technology and large networked infrastructure with interconnected medical devices with new digitalized processes and new applications compose and expand the threat vector and attack surface. This type of change affects our ability to protect organizations against cyber-attacks and must be recognized when planning the services and systems.

Adebukola et al. (2022) presents in their research a few emerging cyber security trends in healthcare, which organizations should consider. These trends according to their research are:

1. Medical Cyber-Physical Systems (MCPS) – wearable and implantable systems connected to Internet of Things. These systems might not encompass cyber security features or do not have maintenance in place after introduction and this predisposes these systems to cyber-attacks.
2. Data privacy, data confidentiality and authorization – Loss of sensitive personal information may cause severe consequences in patient care. Cyber security must be aligned with the business and existing risks.
3. Use of cloud services – Recognizing of risks withing cloud computing and understanding the attack vectors causing the threats. Data must be protected both at rest and in transit.
4. Increasing usage of health applications - Using multiple, partly inadequate applications lacking proper security features in healthcare and administrating sensitive information in those applications compromises' organizations security and patients' confidentiality.
5. Insiders – Insiders, the employees or contractors who have access to the environment and systems may cause cyber threats when being indifferent or not aware of procedures or policies or not trained against cyber security threats.

Interestingly Mattioli et al. (2023) ENISA exercise report "Foresight on emerging and future cybersecurity threats 2030" is covering threats emerging to 2030 and some of these threats can be combined with the trends Adebukola et al. (2022) announced with the exception, that Mattioli et al.

(2023) report does not directly link with healthcare services. Cyber-physical systems are considered as risks in 2030 as the amount of IoT devices will increase dramatically according to the report and lack of expertise might lead to unmanaged situation with cyber incidents. Increasing usage of health applications was one emerging trend according to Adebukola et al. (2022). It can be connected to Mattioli et al. (2023) report's threat vector of IoT devices being connected to mobile devices and users communicating through applications of which attackers might try to exploit using vulnerabilities in software. Threats in respect of health information were seen as risks in both studies.

Considering of these trends Adebukola et al. (2022) have introduced and comparing these to the earlier ENISA report of Smart Hospitals in 2016, Bhuyan et al. (2020) research, Digital Pool (2020a) report and Mattioli et al. (2023) report, we can see similarities how organizations should observe and recognize threats in their operations. All these reports indicate the need to understand the operational environment and what the business organizations are working on. As stated, cyber security risk management must be aligned with the business to be comprehensive and have continuity.

5.3 Cyber security supply chain risk management

Digitalization, as described in chapter three, concerns the whole healthcare industry including the pharmaceutical services in hospitals. Digital processes and operations are used to produce real time and formal, reproducible service to control operational risks in production. Parts of these processes and operations are delivered by the suppliers' organizations are related to. Boyens et al. (2021) mentions in their publication, that cyber security incidents are associated with supply chain risks. These incidents are not decreasing according to their study, and organizations affected with this challenge do not yet have clear methods of how to handle these risks caused by supply chain. Risk management concerning supply chains and cyber security risks is called Cyber Supply Chain Risk Management, C-SCRM.

Recognizing and understanding of the supply chain, which can be layered in organizations different operations, is the key for successful cyber security supply chain risk management. Within remarkable digital operations and layered supply chains the cyber security risks increase. Supply chains not only include the suppliers of the services or products to the organization but can also include the customers and subcontractors in such cases when the organization manufactures and delivers products or services to its clients. The losses and impacts which can affect the pharmaceutical service supply chain and the operations of the hospital pharmacy, can be extremely serious including the loss of life or compromising the business continuity (Boyens et al. 2021). Muthuppalaniappan and Stevenson (2021) addresses in their article "Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health", healthcare supply chains to be vulnerable to cyber-attacks and experience absence of resources, which might lead to continuing issues with recovering to normal state.

Solfa (2022) in his research "Impacts of Cyber Security and Supply Chain Risk on Digital Operations: Evidence from the Pharmaceutical Industry", expresses that digitalization of processes only does not increase cyber security risk level itself but instead supports organization's ability to manage risks emerging from supply chain. This research indicates, that increase of digital services in pharmaceutical industry can improve organization's ability to control business processes, share information more productively or protect data and formulas, and eventually control cyber security risks better.

In Digital Pool (2020b) study mentioned earlier, digitalization is mandatory for businesses. According to this study and research publications from Boyens et al. (2021) and Solfa (2022), these all studies indicate the importance of understanding of the supply chains in place. This is the foundation for cyber security supply chain risk management. Boyens et al. (2021) publication expresses the key functions that many companies and organizations could benefit from as guidance for continuous C-SCRM program. These key functions and the meaning by their publication, are:

- Accommodating C-SCRM thru the organization
    - Accommodating Cyber Supply Chain Risk Management thru the organizations signifies organization ability and maturity to process cyber security as part of supply chain risk management and recognize cyber security as one element of comprehensive risks management procedure.
- Authorizing C-SCRM program in the organization

  - Establishing C-SCRM program in the organization includes utilization of policies, procedures, processes, and tools with governance model for managing the C-SCRM program. The governance model should include the responsibilities and roles inside the organization aligned with the other risk management responsibilities.
- Recognizing and controlling critical components and suppliers
  - Organization must identify their operational environment including assets, processes, critical functions, data, and systems which have dependencies with suppliers either by access to the organizations systems and data or delivery of systems and infrastructure as a service to the organization.
  - Suppliers need to be recognized both to manage risks and to register supplier criticality.
- Understanding the supply chain
  - Supply chains can be exceedingly long, and an organization must understand the whole chain to be able to assess cyber security risks emerging from the supply chain.
- Cooperating firmly with key suppliers
  - Increase of formal cooperation between key suppliers and organization improves coordination of the supply chain and promotes the maturity of C-SCRM.
- Encompassing key suppliers in resilience and development activities
  - Organization's resilience against cyber threats must be aligned with the business objectives and supplier chain affecting the business must be included into organization contingency planning.
- Assessing and monitoring throughout the supplier relationship
  - Organizations should monitor their supplier through the relationship to control risks and to recognize changes in supplier cooperation depending on supplier's criticality to organization's business.
- Planning for the complete life cycle of the solutions.

- Organizations must protect their business by preparing for accidental disruptions in the supply chain. Business continuity must be protected with a systematic approach to contingency planning and disaster recovery (Boyens et al., 2021).

5.4 Risk management in case organization

Administrative regulations direct the case organization to control risks in proper manners and authorize and set responsibilities for risk management. Organization management (Figure 4) is responsible for organizing risk management in the range of managers responsibility. All employees are responsible for reporting and notifying risks they recognize using procedures implemented to this purpose. The Chief Risk Officer was nominated for common risk management development and coordination to ensure continuous and analogue procedures in risk management throughout the organization. Cyber security risk management is covered by information security function. Information security is part of the information management division supervised by the Chief Information Officer. The organization has appointed an Information Security Officer to develop and coordinate information security and cyber security and Data Privacy Officer to develop and coordinate data privacy. Data privacy and information security are managed by separate divisions.

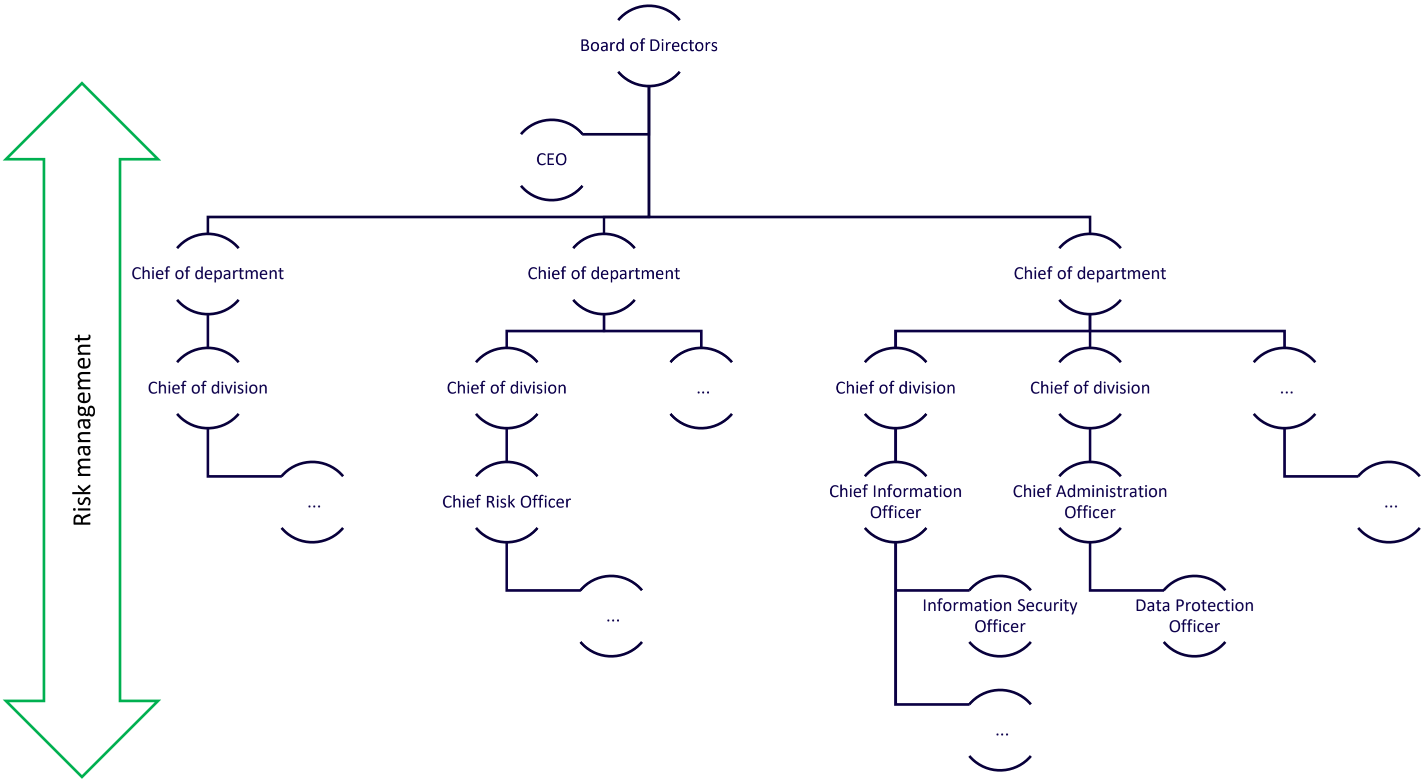


Figure 4, Organization management model

5.5 Using standards and frameworks

In chapter 4.1, we expressed the reason for risk management, which is to coordinate activities to control existing risks (ISO/IEC 31000:2018, 2018). Discussion in chapter 4.2 indicates, that cyber security risk management should be comprehensive, business aligned approach covering both technical and human factors. Understanding of an organization's operational environment, including supply chain arrangements, is crucial for implementing appropriate countermeasures.

Duncan and Whittington (2014) announce in their article, that international standards and legislation are implications of certain time and reasons but might not cover organizations’ current threat environment because of constantly evolving technology solutions. They express the fact that implementing the requirements of standard does not automatically guarantee the security of the organization. According to Al-Ahmad and Mohammad (2013), large amount of cyber security frameworks, standards and best practices are published to help organizations to manage and develop their cyber security risk management, but it is not obvious which one to use in their own environment. Their study focuses on analyzing most common standards and frameworks existing in 2013 and the study was covering ISO 27001, ISO27002, ISO 27005, ITIL, COBIT, Risk IT, Basel II, PCI-DSS and OCTAVE. They emphasize in their article literature missing studies which organizations could benefit from when choosing applicable approach to cyber security risk management (Al-Ahmad & Mohammad, 2013).

According to the discussion of adopting standards and frameworks and referring to chapter 5.2, in which presented studies expressed the need of understanding organization operations and environment, technologies and human factor, supportive research question one (1) “How can we achieve consistent cyber risk management model for hospital pharmacy promoting risk management and cyber security management frameworks and standards? “ becomes relevant. Additionally, Duncan and Whittington (2014) presented in their study that one criterion is not appropriate for all businesses and organizations.

In this study, only a few standards and frameworks are presented. As discussed, the use of standard or framework is not straightforward option due to variety of choices and should relate to the organization ability and target with risk management or more specific cyber security risk management. Included standards and frameworks are

- The Operationally Critical Threat, Asset, and Vulnerability Evaluation, (OCTAVE) methodology
- ISO/IEC 27001:2022, *Information security, cybersecurity and privacy protection - Information security management systems - Requirements*
- ISO/IEC 31000:2018, *Risk management - Guidelines*
- National Institute of Standards and Technology (NIST) Cybersecurity Framework
- Cybermeter – Kybermittari.

5.5.1 The Operationally Critical Threat, Asset, and Vulnerability Evaluation, (OCTAVE) methodology

Caralli et al. (2018) introduce technical report of the next generation OCTAVE method, OCTAVE Allegro. OCTAVE Allegro is an evaluation method for critical threats, assets, and vulnerabilities, which offers a consolidated approach to information risk management process to businesses for ensuring resiliency. This framework integrates people, technology, and facilities related to information and business processes and should help organizations to achieve results with narrow resources. OCTAVE Allegro includes example risk assessment worksheets and questionnaires which can be used as a template for own purposes. OCTAVE Allegro method has four (4) categories and eight (8) steps to perform by assessment person or team. Category one (1), Establish Drivers, is for establishing risk measurement criteria. Category two (2), Profile Assets, consists of two (2) steps; Information Asset Profile Development and Identifying of Information Asset Containers. Category three (3), Identify Threats, includes also two (2) steps, Identifying Areas of Concern, and Identifying Threat Scenarios. The fourth (4) category, Identify and Mitigate Risks, introduces three (3) steps, which covers risk identification, risk analysis and risk mitigation methods (Caralli et al., 2018).

5.5.2 ISO/IEC 27001:2022

ISO (the International Organization for Standardization) / IEC (International Electrotechnical Commission) 27001 is an international standard for information security management system. With this systematic approach to information and cyber security management practices, organizations can develop information security management system according to their needs. The standard emphasized the importance of risk management within information security management system for retaining confidentiality, integrity, and availability of data. It requires organization to implement and document processes to address and manage information security risks (ISO/IEC 27001:2022, 2022).

Information security controls (organizational, people, physical and technological) are presented in ISO/IEC 27002:2022 standard but presented also in Annex A chapter of the ISO/IEC 27001:2022. The standard adduces information security controls which organizations can implement according to their requirements but does not offer technical solutions directly.

ISO/IEC 27001:2022 requires organizations to develop information security management system continuously and tend to corrections of any occurring nonconformities. Corrective actions must comprise reaction against nonconformity, confirm nonconformity not recurring, apply needed actions, ensure the efficiency of corrective actions implemented, and revise of the information security management system when applicable (ISO/IEC 27001:2022, 2022).

Information Security Management System (ISMS) is one approach to cyber security risk management combined with other ISO/IEC27 -series standards. This approach is comprehensive and requires resources and does not separate businesses. It requires commitment from the organization to implement and maintain the ISMS effective and suitable for organization needs. ISO/IEC 27001:2022 (2022) offers tools for many organizations for cyber security management and controls against common information security vulnerabilities in the areas of organizational, people, physical and technological security and it emphasizes the importance of understanding organizations operational environment (ISO/IEC 27001:2022, 2022).

5.5.3 ISO/IEC 31000:2018

ISO/IEC 31000:2018 (2018) is not a standard for cyber security risk management but it is worth mentioning. This standard is to support organizations towards better organized risk management and can be utilized within all businesses and all functions of an organization when facing risks. This standard describes the actions for the comprehensive risk management process including risk identification, risk analysis and risk evaluation (ISO/IEC 31000:2018, 2018).

5.5.4 National Institute of Standards and Technology (NIST) Cybersecurity Framework

NIST has created Cybersecurity Framework for organizations to help their process towards professionally managed cybersecurity program. Cybersecurity Framework consists of five main elements to cyber risk management which can be used to improve both knowledge and organization procedures for cyber risk management (Figure 5). The elements include

- Identify – This element improves organization understanding of its environment, critical processes, and assets. It guides towards to comprehensive management of cyber security procedures by recommending of implementation of information and cyber security policies, incrementing the knowledge of the data usage and storage, maintaining timely catalogue of software and hardware assets, and delivering risk assessment against the assets identified.

- Protect – This function is for ensuring the availability of the critical services identified in the previous step. Implementation of access management, backups, device and sensitive data protection, end user training and vulnerability management for devices are key tasks to be performed under this element.
- Detect – To be able to deliver continuous service production to the organization, detecting and correctly identifying anomalies, cyber security events and consequences is crucial task to perform.
- Respond – When cyber security event happens, organization should be able to respond with planned countermeasures to the event. This function guides an organization to rehearse and test its countermeasure capabilities and procedures against cyber security events.
- Recover – Organization should be able to recover from the cyber security event. To manage to recover, organization must maintain recovery plans for systems and services. This element of the Framework promotes communication with stakeholders. NIST notifies that organizations address their cyber security risks differently and risks vary between organizations and the Framework does not change this approach of risk management (Cybersecurity, C. I., 2018).

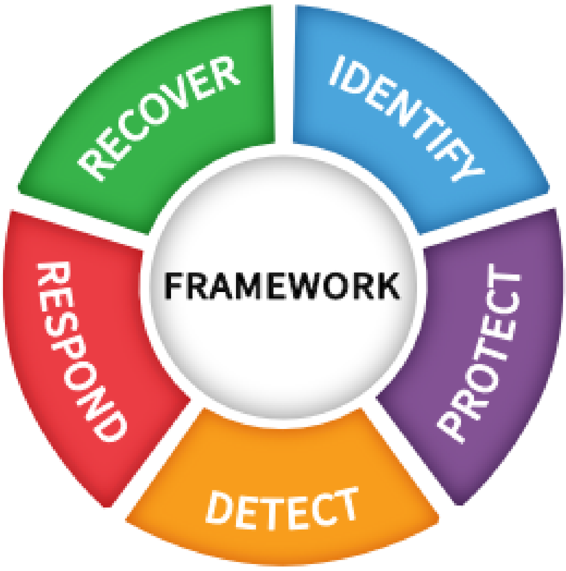


Figure 5, NIST Framework (Cybersecurity, C. I., 2018)

To the context of this research, NIST Cybersecurity Framework contain essential elements to be considered not forgetting the human or social factor and end user training, which was discussed earlier in chapter 4.2. This Framework delivers five basic elements to the cyber security risk management process but does not include technical solutions itself. All the elements of this Framework are divided into categories, which present more detailed tasks for organizations to perform. All presented tasks are mapped with other related cyber security reference materials with accurate actions. NIST Cybersecurity Framework is not a simplified approach to cyber security risk management but offers an extensive range of information for an organization to use when improving their own cyber security risk management processes and procedures.

NIST Cyber Security Framework introduces ISO/IEC 27001, CIS Controls, COBIT, NIST SP-800-53 Rev4 and ANSI/ISA-62443-3-3 (99.03.03)-2013 as their reference information for the detailed actions of each task in categories (Cybersecurity, C. I., 2018).

5.5.5 Cybermeter - Kybermittari

Cybermeter was developed by the National Cyber Security Centre (NCSC-FI) and it is targeted mostly for cyber threat management for companies and organizations working on critical industries. Cybermeter is not a standard or framework rather than a comprehensive tool for cyber threat management. According to the National Cyber Security Centre (2023), Cybermeter has implications both from NIST Cyber Security Framework and Cybersecurity Capability Maturity Model (C2M2). This tool can be used in Finland for national cyber security situation awareness improvement when users send their own assessment results back to NCSC-FI and improving own cyber security management practices inside organizations. Use of Cybermeter tool is not related to any standard or framework companies or organizations have adopted as part of their own cyber security threat management (The National Cyber Security Centre, 2023).

According to The National Cyber Security Centre (2023), Cybermeter includes ready to use cyber security risk and threat assessment tools covering eleven (11) areas of cyber security. Protection of Critical Services, area one (1), covers identification and governance of critical services and minimizing impacts of cyber security incidents. Second area (2), Asset, Change, and Configuration Management, includes management actions for organizations' critical assets. Third area (3), Threat and Vulnerability Management, includes actions for cyber security threats and vulnerabilities detection, identification, analyzing, managing, and responding. Fourth area (4), Risk Management, is to emphasize enterprise level risk management program for identifying, analyzing, and responding to the cyber security risks facing the organization. Area five (5), Identity and Access Management, is to control both physical and logical access, management and control of identities and management actions for proper formalities of access management. Situation Awareness, area six (6) in Cybermeter, comprises logging and monitoring actions to collect information from cyber security situation and from organizations' operations. Area seven (7), Event and Incident Response and Continuity of Operation consists of management actions for cyber security event detection, analyzing and responding. Risk Management for Third Parties, area eight (8), provides actions for supplier and other third-party cyber security risk management, which could affect organizations' critical infrastructure and services. Area nine (9), Workforce Management, focuses on personnel and cyber security culture in organization. It promotes cyber security responsibilities assignment, employee training, awareness programs and management actions towards consistent cyber security culture. Cybersecurity Architecture, area ten (10), presents cyber security architecture strategy and controls for network, data, software, and IT & OT assets and management actions for achieving inherent, consistent working culture. Area eleven (11), Cybersecurity Program Management, is for describing organizations' own objectives within cyber security (The National Cyber Security Centre, 2023).

The Cybermeter tool is an extensive approach to cyber security threat management and organization can take either all areas of it or then use only areas that are seen important from the organization point of view.

5.6 Legislation

According to the Constitution of Finland (731/1999) and European Union, Charter of Fundamental Rights of European Union (2012, 391, article 7), everyone’s right to the protection of private life is a fundamental right. In the operation of public organizations, the Act on the Openness of Government Activities (621/1999) applies to the authority's activities. It determines publicity of the authority's documents as primary option unless confidentiality limits the publicity. The Wellbeing service counties including the case organization are obligated to constitute an Information Management Unit by each. These Information Management Units must secure a sufficient level of data protection and information security in the operations of public organizations (Act on Information Management in Public Administration, 906/2019). According to the case organization’s internal policies, the most important regulations governing information security and data protection include

- The Constitution of Finland (731/1999)
    - 2:10 § (Privacy life and the secrecy of confidential communication)
    - 2:12 § (The publicity of the documents of the authority)
- Regulation (EU) 2016/679 of the European Parliament and of the Council, on the protection of natural persons in the processing of personal data and on the free movement of this data and the repeal of Directive 95/46/EC (General Data Protection Regulation)
- Data Protection Act (1050/2018)
- Health Care Act (1326/2010)
- Act on Health Care Professionals (559/1994)
- Laki sosiaalihuollon ammattihenkilöistä [Act on Social Care Professionals] (817/2015)
- Sosiaali- ja terveysministeriön asetus potilasasiakirjoista [Decree of the Ministry of Social Affairs and Health from patient documents] (94/2022)

- Laki sosiaalihuollon asiakasasiakirjoista [Act on Social Care Customer Documents] (254/2015)
- Laki sähköisestä lääkemääräyksestä [Act on Electronic Prescription] 61/2007)
- Act on the Openness of Government Activities (621/1999)
- Act on the Status and Rights of Patients (785/1992)
- Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (784/2021)
- Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista (812/2000)
- Arkistolaki [Archive Act] (831/1994)
- Employment Contracts Act (55/2001)
- Tort Liability Act (412/1974)
- Act on the Protection of Privacy in Working Life (759/2004)
- Laki sosiaali- ja terveystietojen toissijaisesta käytöstä [Act on Secondary Use of Social and Health Information] (552/2019)
- Laki eräistä EU-direktiiveissä säädetyistä lääkinnällisistä laitteista [Act on certain medical devices regulated in EU directives] (629/2010)
- Medical Devices Act (719/2021)
- Act on Information Management in Public Administration (906/2019)
- Rescue Act (379/2011)
- Criminal Code (39/1889) 38 §
- Laki kunnan ja hyvinvointialueen viranhaltijasta [Act on the office holder of the municipality and the welfare area] (2003/304)
- Act on Electronic Communications Services (917/2014)
- Laki hyvinvointialueesta [The Act on the Wellbeing County] (611/2021)
- Laki sosiaali- ja terveydenhuollon järjestämisestä [Act on the organization of social and health care] (612/2021)

6 Data collected – documentation, questionnaire, workshops and interviews

6.1 Current state analysis

As described in chapter 2.1, this research is based on the actual development need for cyber security risk management on pharmaceutical service supply chain digital operations in hospital pharmacy. Current procedures with cyber security risk management must be developed according to the business and the constantly evolving threat matrix. It was identified that there is a gap between cyber operations and the pharmaceutical service supply chain digital operations. Current state analysis was done to address the missing procedures from pharmaceutical service cyber risk management perspective. The analysis was based on existing documentation described in chapter 2.2.1.2 Documentation.

Documentation and procedures were developing simultaneously but independently with this study. This can be explained with changes in case organization during the thesis process. Organization has experienced major changes with its operations, processes, and procedures including changes with policies and guidelines and started operations 1st of January 2023.

Observations from the documentation are, that pharmaceutical services are covered corresponding other case organization operations but do not offer any tools for pharmacy personnel for cyber risk management or recognizing threats or risk in daily operation. Pharmaceutical services are critical services of the welfare counties. Considering this, procedures, and principles for more accurate cyber security risk management for these services are well rationalized.

Risk management organization is in place and responsibilities are set. Cyber security policies and procedures have been accepted by the management board and signed by the director of the welfare county. Cyber security is covered by the information security office and data protection officer is nominated. Physical security is managed by a nominated Security Manager part of the risk management office. External parties are being used for delivering ICT services and cyber security services for the case organization. Cyber security services include technical support, consultancy, and security operation center services.

6.2 Questionnaire

The questionnaire described in chapter 2, Research approach and methods, was used to collect information from the case organization pharmacy employees in accordance with secondary research questions “How do the hospital pharmacy personnel understand and experience cyber security risks in their daily operations?”. The questionnaire was sent to 75 employees from which 16 employees returned the questionnaire with answers and results were analyzed using classification method. The link to the questionnaire was delivered to the pharmacy personnel by the dedicated person in the pharmacy. Answers are anonymous and represent employees’ own sentiments of each question.

6.2.1 Open answer questions

The first questions were to perceive how employees undergo their responsibilities regarding cyber security risks and threats and how they experience their abilities to recognize cyber security risks. All 16 participants indicated recognizing cyber security threats and risks belonging to their normal duties and nine (9) out of 16 answers stated lacking expertise or opportunities to be able to recognize cyber security risks.

The question of existing cyber security risks related to pharmaceutical services digital supply chain was answered by 15 participants of which 12 included named digital services and systems used for pharmaceutical services.

How cyber-attack against pharmaceutical services digital supply chain could affect to the case organization operation was answered by 15 employees of which 14 participants estimated various severe challenges with pharmaceutical services and one (1) could not nominate any specific aspect.

What kind of methods should be used to recognize and control cyber security risks related to participants’ duties superior to current situation was answered by 15 participants of which seven (7) indicated the need for more information and training to the personnel and four (4) could not nominate any specific method. Last four (4) from 15 were singular answers.

The question of having more training to be able to recognize and understand cyber security threats got 16 answers of which 14 indicate the need for more training, one (1) does not know and one (1) does not need more training.

6.2.2 Closed answer questions

The first multiple answer option questions were to get information, how participant experience presented answer choices to be connected to cyber security risk management of pharmaceutical services. Results show that participants 100% recognize information security and data privacy training, up-to-date access rights management and information security and data privacy policies as part of cyber security risk management practices. Seventy-five percent indicated information technology systems related to pharmaceutical supply chain and 81% denoted suppliers' remote connections to organizations information systems to be connected to pharmaceutical services cyber security risk management. Answers covering 44% considered contract management and 56% indicated cyber security management system to be part of pharmaceutical services cyber security risk management. Interestingly over 90% considered the use of internet at work and the use of email at work to be connected to pharmaceutical services cyber security risk management practices. Cyber security requirements for purchases and up-to-date documentation of ICT-infrastructure were considered by 63% of the participants.

The second multiple answer option question was to collect information, how participant specifies the need of improving the cyber security risk management in case organization. All 16-participants answered to the questionnaire were solid with their answers and indicated 100% need for additional cyber security risk management training for employees. Clear instructions and procedures for recognizing risks and managing those were selected by 88% and 81% would deliver regular risk assessment in their unit. Twenty-five percent would increase management responsibility and supplier management as part of cyber security risk management improvements. Expanding resources in information and cyber security was selected by 50% and 31% would increase employees' responsibilities as cyber security risk management improvement methods. The change of purchase process for new systems was selected by 31%.

The last multiple answer option question collected information of the need to improve information and cyber security procedures in the case organization and offer claims, how improvements could be made. Fifteen participants answering this question selected the training for recognizing and managing information and cyber security risks and clear procedures for employees to follow in their own work to recognize cyber security risks. Increase of responsibilities to information and cyber security personnel was selected by 53% of the answers and same amount would also increase resources in information and cyber security. Outsourcing of information and cyber security function was selected by 27% and 40% would increase employees' responsibilities. Adding comprehensive instructions and guidelines to the organization intranet for observing cyber security threats and risks management was selected by 60% and 13,3% would acquire additional information system for reporting purposes.

6.3 Workshop one: Defining pharmaceutical service supply chain

Workshop one was held on 23rd of May 2023 in the hospital pharmacy premises with the pharmacists (three invited, two participated) and the researcher. The goal of this workshop was to understand and draft a model of existing pharmaceutical supply chain model for hospital pharmacy. During the workshop participants were discussing and analyzing pharmaceutical supply chain structure in case organization. Participants were invited to the workshop by email calendar invitation, in which they received a description of the study and goal of planned workshop and working model. Participation was based on their voluntary to contribute time and knowledge for this study. The workshop was kept in good spirit with an open-minded and objective attitude. The researcher reminded participants that all the results will be handled without any personal information.

Based on the information gathered during the workshop, simplified structure for pharmaceutical service supply chain for hospital pharmacy is described in figure six (6). The structure of pharmaceutical supply chain for hospital pharmacy includes five (5) steps according to the information gathered in workshop. These steps are

1. Wholesale dealers: The case organization has multiple wholesale dealers which deliver different types of pharmaceutical ingredients.
    a. Wholesale dealers are controlled / approved by Fimea

2. Distribution center(s): Distribution centers for logistics and delivery of pharmaceutical ingredients to customers.
3. Acquiring the pharmaceutical ingrediency / Hospital pharmacy: Responsible for delivery of pharmaceutical services under Medicine Act 395/1987
4. Local storage: Storage of medicines. Hospital pharmacies are obligated to store certain pharmaceutical ingredients according to the Act of Mandatory Reserve Supplies 979/2008.
5. Delivery: Internal and external deliveries of pharmaceutical ingredients

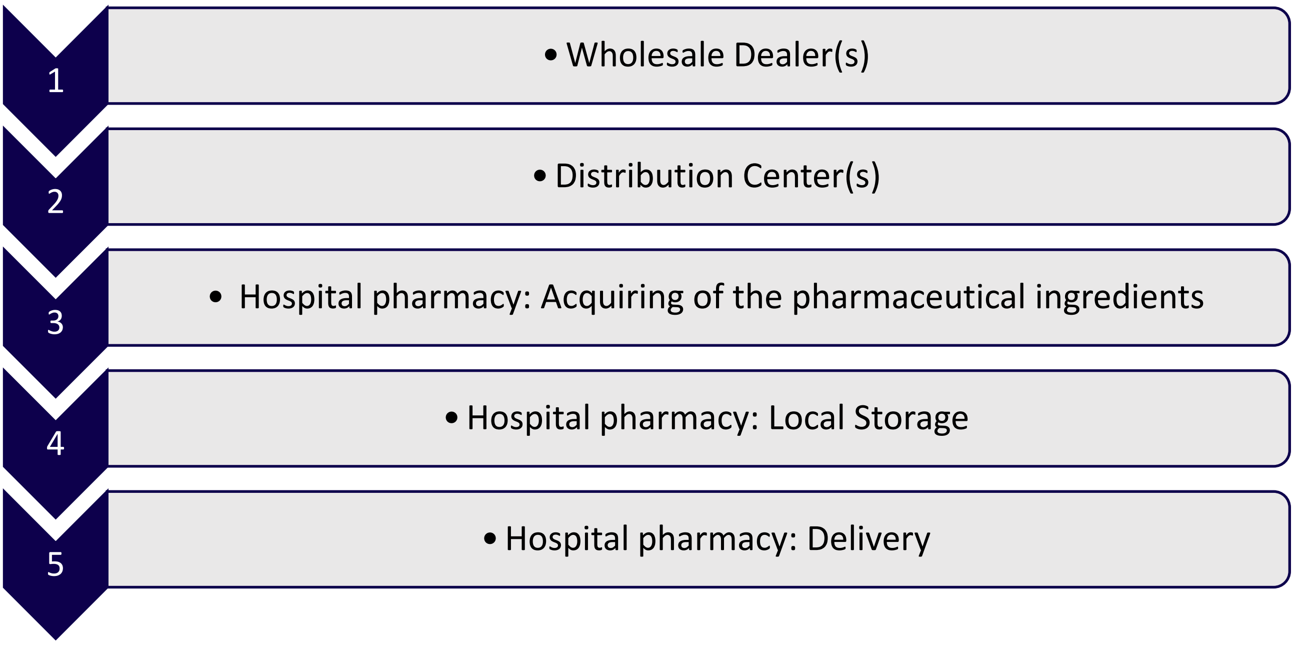

1
• Wholesale Dealer(s)
2
• Distribution Center(s)
3
• Hospital pharmacy: Acquiring of the pharmaceutical ingredients
4
• Hospital pharmacy: Local Storage
5
• Hospital pharmacy: Delivery

Figure 6, Simplified structure of pharmaceutical supply chain for hospital pharmacy

As on observations from the workshop one, the pharmaceutical supply chain structure is understood superbly by the participants. Cyber security is not controlled in any pharmacy or pharmaceutical service specific authorities, or legislation and cyber security management should be connected more deeply with pharmaceutical services in case organization.

6.4 Workshop two: Describing digital services of the supply chain

Workshop two was held on 25th of May 2023 in the hospital pharmacy premises with the pharmacists (three invited, two participated) and the researcher. One additional participant was invited to join by the original participants. Workshop two comprised discussion and analyzing pharmaceutical supply chain digital services structure in case organization between participants. The goal of this workshop two was to understand digital services used in the pharmaceutical supply chain and cyber security threats evolving from the digital services. Original participants were invited to the workshop by email calendar invitation, in which they received a description of the study and goal of planned workshop and working model. Participation was based on their voluntary to contribute time and knowledge for this study. The workshop was kept in good spirit with an open-minded and objective attitude. The researcher reminded participants that all the results will be handled without any personal information. Additional participant was also briefed on the aim of the study and the goals of the workshop.

As a starting point for the discussion, the model from the first (1.) workshop was used. During the second (2.) workshop, participants discussed and analyzed the weaknesses, strengths, and importance of the supply chain structure including the digital services. They were able to recognize information technology assets, systems used for pharmaceutical services, automation systems, OT systems, relations to other local information technology environment, networks and Enterprise Resource Planning system used for order, storage, inventory, and delivery -information management (Figure 7).

Discussion of the assets and systems used in hospital pharmacy led participants to consider threats and vulnerabilities regarding the supply chain structure limited to the assets and systems used in or for hospital pharmacy operation. There are multiple information and automation systems and several suppliers for those systems. All these systems are part of the overall supply chain and during the workshop, some critical services and systems were recognized. Part of the services were categorized as “important / supportive” but not critical. Interruptions with this category systems can create unfortunate situations in operation and cause delay but do not compromise hospital pharmacy service production.

Relations for other hospital information technology systems were discussed as part of the workshop agenda. The workshop introduced dependencies between the hospital pharmacy operations and other hospital ICT environment.

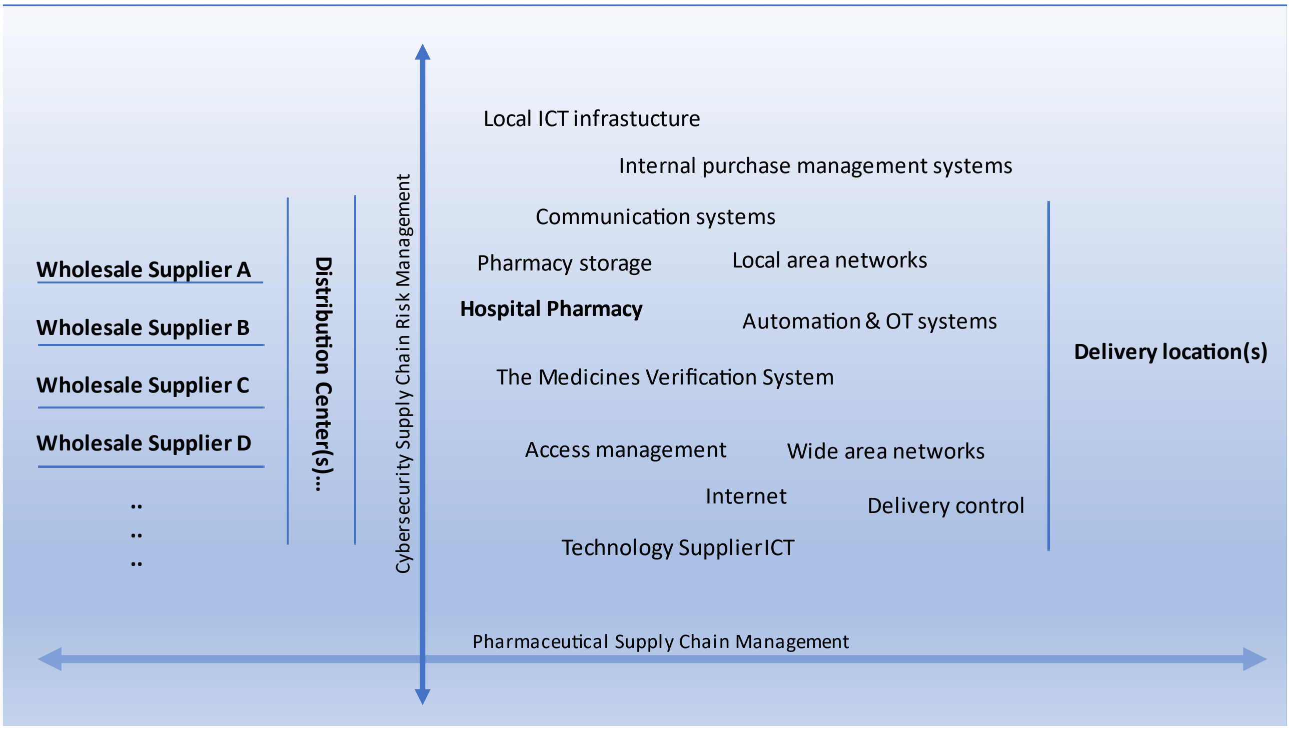


Figure 7, Digital services as part of pharmaceutical supply chain in case organization

As an observation, it was clearly agreed between participants that cyber security risk management is an important part of securing the resiliency of pharmaceutical services and continuity of hospital pharmacy operations. This workshop addressed that current cyber security risks management is not continuous and does not cover pharmaceutical service operation comprehensively.

6.5 Interview one (1)

Interview one (1) was held on 29th of May 2023 both using Microsoft Teams and on-site in the meeting room. Two participants were invited to the meeting. These participants represent senior ICT expertise and are involved in hospital pharmacy ICT services. One participant represents the case organization ICT department and one service provider, which delivers ICT services to case organization. Both participants were invited using email calendar invitation. They were told that participation in this interview is fully voluntary, and they can leave any time without any consequences. Participants were informed of the aims of this study and no personal information will be used. This group interview was to validate findings from workshop two and make supplements for existing model if necessary. Researcher and one participant were in the meeting room and Teams meeting was used with the other participant.

Models from the first and second workshops were presented to the participants, and they discussed and analyzed presented models against the conferred questions. Participants discovered the presented model missing a few essential elements and suggested these to be added as part of the ICT infrastructure. They were able to confirm systems used as part of pharmaceutical services supply chain gathered from workshop two. Both participants appraised cyber security risks emerging from the ICT infrastructure and are relevant for the hospital pharmacy. They denoted the importance of ICT services management and accurate ICT asset management as part of cyber security risk management. Both participants considered supplier management and contracts as important parts of supply chain management.

In addition to Figure 6 from workshop two (2), new systems were introduced as part of digital services in pharmaceutical supply chain. These systems are integration platforms, financial management system and invoicing systems. Systems were added to the list of ICT systems and are presented in figure 8.

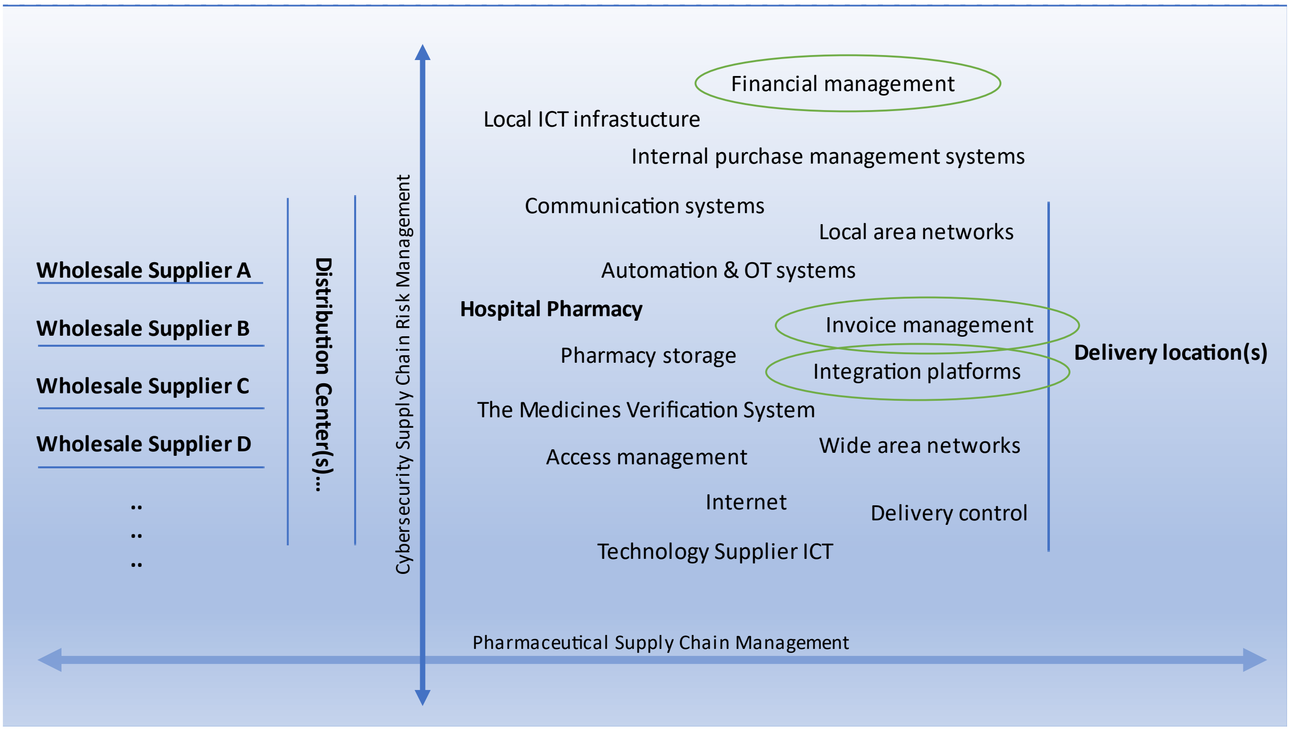


Figure 8, Digital services as part of pharmaceutical supply chain in case organization # additional systems

As an observation from the first group interview, communication between ICT personnel, cyber security personnel and pharmacy personnel should be increased to be able to monitor and control cyber security threats deriving from the changes in ICT environment.

6.6 Workshop three (3)

Workshop three (3) was held on 8th of June 2023 in the hospital pharmacy premises with the pharmacists (three invited, two participated) and the researcher. During this workshop, participants were analyzing threats, vulnerabilities, and consequences regarding digital services in pharmaceutical services. The goal of this workshop three was to get an understanding of cyber security risks evolving from the digital services in pharmaceutical supply chain structure. Participants were invited to the workshop by email calendar invitation, in which they received a description of the study and goal of planned workshop and working model. Participation was based on their voluntary to contribute time and knowledge for this study. The workshop was kept in good spirit with an open-minded and objective attitude. The researcher reminded participants that all the results will be handled without any personal information.

Information collected from the earlier workshops and interviews of the critical infrastructure and systems used in hospital pharmacy for pharmaceutical service production were used. Before the actual workshop, the first draft of the risk assessment table was created, and this was given to participants before this workshop. During this workshop, threats, vulnerabilities, and risks were analyzed estimating likelihood and consequences (impacts) for operations. New vulnerabilities were found for presented threats and 26 risks (Table 1) were recognized of which one (1) was categorized as critical risk, seven (7) major risks, 16 moderate risks and two (2) minor risks.

Table 1, Risk assessment workshop three (3)

Risks totally found 26		
Critical risks	1	4 %
Major risks	7	27 %

Moderate risks	16	62 %
Minor risks:	2	8 %

In this assessment, the risk event describes occurrence or change of a particular set of circumstances and risk event can have multiple causes and consequences (impacts) and can affect multiple objectives (ISO/IEC 31000:2018, 2018). Each risk was valued using scores from one (1) to four (4) both for likelihood (Table 2) and consequences (Table 3). Smaller numbers under “Rating” column describe smaller likelihood and smaller impact. Higher number under “Rating” column increases the likelihood and consequence

Table 2, Likelihood ratings and descriptions

Rating	**Description**	**Definition**
4	Almost certain	85 % or greater change of occurrence over life of asset
3	Likely	50% up to 84% change of occurrence over life of asset
2	Possible	15% up to 49% change of occurrence over life of asset
1	Unlikely	1% up to 14% change of occurrence over life of asset

Table 3, Consequence ratings and descriptions

Rating	**Description**	**Definition**

4	Critical	• Service not operational • Long service downtime possibility • High-cost effects • High reputation loss possibility
3	Major	• Remarkable service effects • Service partly operational • Remarkable cost effects • Reputation loss possibility
2	Moderate	• Moderate service affects • Delays possible • Moderate cost effects • Moderate reputation loss possibility
1	Minor	• Minor service affects • Minor cost effects

As an observation from workshop three (3), cyber security risk assessment is new to the hospital pharmacy personnel. Threats and vulnerabilities were understood but risk assessment was experienced too “difficult” when estimating threats, vulnerabilities, likelihood and consequences for each threat and vulnerability. Cyber risk assessment should be conducted by cyber security personnel with pharmacy personnel, when using threats – vulnerabilities – consequences -model for the assessment.

6.7 Interview two (2)

Interview two (2) was held on 20th of June 2023 using Microsoft Teams. Three (3) participants were invited to the interview. Participants represent senior ICT expertise and are involved in hospital pharmacy ICT services. One participant represents the case organization ICT department and two work for service provider, which delivers ICT services to case organization. Participants were invited using email calendar invitation. They were told that participation in this interview is fully voluntary, and they can leave any time without any consequences. Participants were informed of the aims of this study and no personal information will be used.

This group interview was to validate found risks from workshop three and make supplements if necessary. Questions were presented to the participants concerning the created risk assessment model, criticality of the ICT systems, contingency planning, and relations between ICT systems.

During this interview, participants confirmed the findings from the earlier risk assessment and the total amount of found risks remained as 26. They argued for some risk calculations and emphasized the value of maintenance and support contracts for critical systems and the relevant asset management. One (1) was categorized as critical risk, seven (7) major risks, 15 moderate risks and two (2) minor risks (Table 4).

Table 4, Risk assessment interview two (2)

Risks totally found 26		
Critical risks	1	4 %
Major risks	8	31 %
Moderate risks	15	58 %
Minor risks:	2	8 %

As an observation from interview two (2), senior ICT expertise is needed for holistic cyber risk assessment in case organization. Their expertise is required to be able to recognize missing elements in ICT contracts or relevant affiliations between systems understanding the fact, that external ICT service providers do not have similar visibility to case organization business than organization itself.

6.8 Interview three (3)

Interview three (3) was conducted on 28th of June 2023 using Microsoft Teams. One participant was invited to the interview by email calendar invitation with the interview subject. Interview was based on participants voluntary, and interview could be stopped at any time if participant so decides.

The goal of this interview was to examine how the executed working method for cyber risk assessment would be suitable to the pharmacy operation or what changes should be made to the process. All the information from the earlier interviews and workshops was available during the interview. The participant expressed the need for clear and uncomplicated way for risk and threat recognition without an expertise for cyber security. Co-operation with ICT and cyber security personnel was expected as well.

As an observation from interview three (3), similarities for earlier workshops and interviews observations are clear. Cyber security risk assessments are experienced difficult to perform and are not integrated as part of daily operations.

7 Designing the risk management model

Chapter five (5) discusses cyber security risk management from the strategy point of view and possible cyber security risks in healthcare and choosing corresponding approach to control risks. Earlier studies express that there is not one standard or framework which could solve cyber security challenges for all businesses as all businesses are different and those all face various threats in their operations. Each business should focus on analyzing their threat vectors, vulnerabilities and risks evolving from the operations (Duncan & Whittington, 2014; Taherdoost, 2022).

Pharmaceutical service is a critical function in case organization including technological solutions, people, and supply chain structures. To control cyber security risks within this complex structure, we must analyze the data assembled from workshops, questionnaire interviews and literature review.

7.1 Human factor and identities

As discussed in chapter 5.2, Nifakos et al. (2021) indicate employees' influence on cyber security underlying human factors and employees' abilities to face information security factors. Adebukola et al. (2022) mention insiders, the employees or contractors who have access to the environment and systems may cause cyber threats when being indifferent or not aware of procedures or policies or not trained against cyber security threats. Bhuyan et al. (2020) stated in their research that end users including both former and current employees have been arranging 48% of the data breaches and only 10% were not deliberately done. The questionnaire for pharmacy personnel revealed the need for cyber security training and their motivation for having more training, which further reflects the results from the cyber risk assessment delivered in case organization. Interview three (3) addressed the need for "simplified" cyber risk management procedure in daily operation. Because employees have a significant role in cyber security incidents even if not deliberately done, human factors and identities must be considered in pharmaceutical services cyber security risk management model.

7.2 Suppliers and supply chain

Supply chain structures are part of the pharmaceutical services. From the hospital pharmacy perspective, there are numerous suppliers delivering information technology, IoT and OT and software solutions and services which can affect pharmaceutical service operation. This was demonstrated in workshop one (1) and two (2). Risks evolved from the supply chain structures were addressed during risk assessment in workshop three (3), interview two (2) and from the results of the questionnaire. A major risk found during risk assessment concerning the supply chain of the digital services must be mitigated to the accepted level in accordance with the case organization. Boyens et al. (2021) denoted in their publication cyber security risks associating with supply chain risks and presented the Cyber Supply Chain Risk Management program (C-SCRM), which was described in chapter 5.3. Similarly, Muthuppalaniappan and Stevenson (2021) indicate healthcare supply chains to be vulnerable to cyber-attacks. Accordingly, ISO/IEC 27001:2022 (2022) Annex A controls 5.19, 5.20, 5.21, and 5.22 instructs organizations to manage, control and monitor information security risks evolving from the suppliers’ and supply chains. Based on these findings' supplier management and supply chain management must be connected to the cyber security risk management model of the pharmaceutical services.

7.3 Technology and networks

Complexity on the information technology infrastructure and the considerable amount of technology solutions were addressed though the workshops and interviews delivered. Relation between systems and dependencies to hospital infrastructure were recognized and risk assessment indicated threats originating from the technological solutions. Argaw et al. (2020) indicates the base of information security to be built upon professionally managed and reliable information technology infrastructure. Additionally, Coventry and Branley (2018) express information technology to be concern for information security because of increment in connected devices, growth in mobile devices and health devices being used outside the hospital environment. Mattioli et al. (2023) report brought out the threat vector of IoT devices in chapter 5.2.1 and Adebukola et al. (2020) present in their research Medical Cyber Physical Systems and use of the cloud services as part of cyber security trends to be recognized. Due to these observations connected to the information and communication technology, technology solutions, devices, networks, and services must be included into cyber security management model.

7.4 Applications and data

According to Adebukola et al. (2022) approximately 90% of security events concern vulnerabilities in software level. This claim is supported by Bhuyan et al. (2020) by indicating that cyber security breaches in systems are consequences of the mistakes made by the developers and remembering the considerable number of applications used in healthcare. Sensitive personal data must be protected using both administrative and technical security measures to minimize risks (Data Protection Act 1050/2018). Data privacy and use of cloud services are mentioned as emerging cyber security trends in research by Adebukola et al. (2022). Mattioli et al. (2023) report specify users communicating through applications of which attackers might try to exploit using vulnerabilities in software. Workshops and interviews revealed the considerable number of used applications and data stored in systems which are needed for the pharmaceutical service operation. The executed cyber risk assessment indicated threats and risks within data and applications which must be controlled with relevant procedures. As a conclusion, applications and data are included into cyber risk management model.

7.5 Physical dimension

Physical dimension cannot be forgotten when discussing cyber security threats and information security risk management. Physical security is required to protect organizations' assets and people from potential threats and prevent attacks leveraging to cyber dimension. This study was not addressing physical security straight but must be considered as part of cyber security risk management method based on mentioned reasons.

7.6 The governance model for pharmaceutical service cyber risk management

As discussed previously and derived from the results of the questionnaire, literature, interviews, workshops, and organization's internal documentation, the cyber security governance model must include human factors and identities, supplier management, devices, applications, data, ICT infrastructure and IoT/OT, and networks to cover pharmaceutical service operation comprehensively in case organization (Figure 9). In chapter five (5) was stated, that cybers security controls and goals need to be aligned with business targets and control implementation should be integrated with management decisions to protect business and tolerate risks. Similarly, according to The Act on

Information Management in Public Administration (906/2019), existing risks should be understood and changes in environment must be controlled. Referring to the research questions of this study, “What kind of method could be used to recognize and manage cyber security risks emerging from the pharmaceutical services supply chain in hospital pharmacy operations? and “How do the hospital pharmacy personnel understand and experience cyber security risks in their daily operations?”, the findings indicate that the method must include both traditional risk analysis to have enough information from the operations and checklists derived from the risk analysis for pharmaceutical service daily operation in hospital pharmacy. With this approach we can produce tools for the pharmaceutical employees and for the senior ICT experts to support pharmaceutical service operations. Inside pharmacy, checklists are an uncomplicated and nimble way to monitor changes in the operations but also to react to evolving threats from the operation, which earlier could not be recognized as comprehensively. Accordingly, checklists offer tools for ICT experts to be used in the recurrent ICT follow-up meetings to react on coming changes to be able to deliver continuous and secure ICT services.

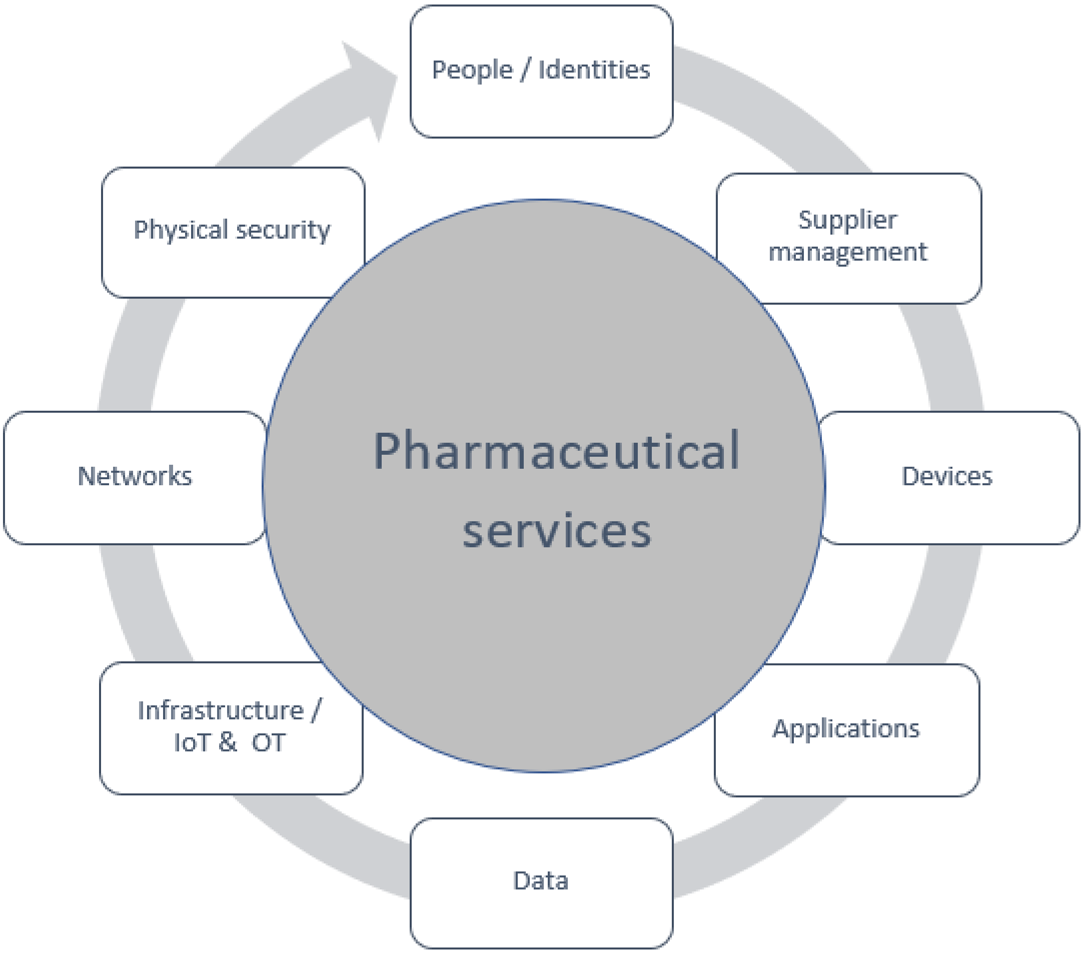


Figure 9, Elements of the pharmaceutical service cyber risk management model

For the secondary research question, “How can we achieve a consistent cyber risk management model for hospital pharmacy promoting risk management and cyber security management frameworks and standards?”, the answer is more complicated. Duncan and Whittington (2014) presented that one criterion is not appropriate for all businesses and organizations. According to Al-Ahmad and Mohammad (2013), despite the numerous cyber security frameworks and standards or best practices, it is not obvious to organizations which one to use in their own cyber security management. The standards and frameworks presented in chapter 5.5 are excellent materials for cyber security risk management and development but do not introduce appropriate tools directly from hospital pharmacy viewpoint. Instead, presented frameworks and standards offer tools for the cyber security and ICT personnel to use for the risk management duties and for organizing comprehensive organization level cyber security risk management and offer models, processes, and procedures which can be utilized in this study. Due to these observations and according to the organizational policies, introduced method is recommended to be integrated with organization level information security management system in case organization to have continuity and visibility.

7.7 Checklists

The eight (8) elements described earlier compose a foundation to cyber risk management for pharmaceutical services in case organization as stated. The elements describe the origins of the risks for pharmaceutical services which must be controlled. Delivered workshops and interviews adduced the need for simplified structure and procedure of managing risks. For this, the checklists were planned as part of cyber risk management. The structure of the checklists remains the same for all mentioned elements and includes both the element and controls required to accomplish the risk minimization. When the change within the element is noticed, the controls must be inspected and if the control does not cover the noticed change, the change must be reanalyzed by the cyber security persons for accuracy of the checklist. The Octave allegro method described in chapter 5.5.1 includes models of questionnaires and worksheets for cyber security risk management but does not include similar checklists. Instead, it offers a concept for using checklists in this study.

The example of the checklist (Table 5) includes the main element, which in this case is: People / Identity. To cover the cyber security risks evolving from the People / Identity -element according to risk assessment delivered which depends on each organizations' guidelines and will for controlling the risks, could include for example:

- Background checks: Are background checks planned for new employees based on the organizational guidelines?
- Non-Disclosure Agreement (NDA): Are all the agreements needed done?
- Orientating a new worker to the workplace: Is orientation accomplished?
- Cyber security trainings: Are trainings completed according to the organizational policies?
- Minimized user access to the systems based on employees' duties: Have we ensured that employee's duties relate to the access rights to the systems?
- What is the motivation of the employees? Have we checked this in annual one-by-one conversations with employees or monthly meetings with the teams to find out the motivation?
- Identities: Have we checked that existing user accounts and identities match with persons working for us?

Checklist can be implemented for example as a table including the main element and the controls needed to manage risk sources in targeted level.

Table 5, Example of the checklist model

Element: People / Identities		
Date:		
Controls / Screening items:	Requirement	Response

		OK / NOK	Not known	Requires new evaluation
Background checks	Background checks must be planned for new employees based on the organizational guidelines			
Non-Disclosure Agreement (NDA)	NDA contract must be done with each employee			
Orientating a new worker to the workplace	Orientation must be accomplished according to organizational guideline			
Cyber security trainings:	Trainings must be accomplished according to the organizational policies			
Minimized user access to the systems based on employees' duties:	Employees' duties must relate to access to the systems. Minimized access rights policy is controlled.			
Motivation	Employees' motivation must be observed using personal and team meetings.			
User accounts / identities	User accounts must expire when the contract ends.			

	User accounts must be based on the contract.			

7.8 Process approach

According to the organization’s internal policies, there is an annual plan for cyber security and data privacy tasks to be performed. Cyber risk assessment for pharmaceutical service is proposed to be included into annual plan for continuity of the cyber risk management. Risk assessment generates controls for the main elements of proposed risk management model which can be used as screening items in checklists for daily operation (Figure 10).

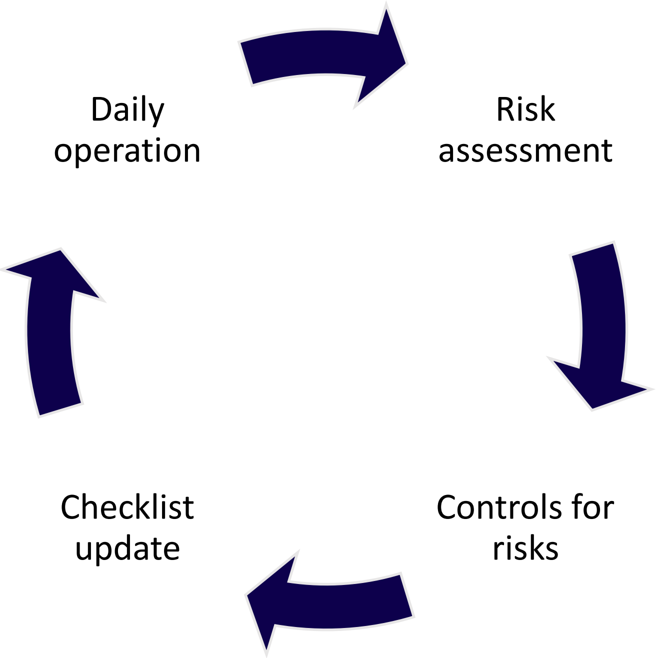


Figure 10, Process approach

The main elements (Figure 8) indicate sources of the risks, which case organization should control. Elements might change if operation changes or when there is some other remarkable change in the operational environment. When a change occurs, new controls are needed, and checklists must be updated. This approach is based on continuous development described in ISO/IEC27001:2022 standard.

7.9 Monitoring criteria

To estimate the functionality of the presented method for cyber risk management in hospital pharmacy environment and for the pharmaceutical service operation, we can set control points. According to the ISO/IEC 31000:2018, (2018) monitoring aims to validate the quality and effectiveness of the process. Research reveals the main risk sources, risk amounts, criticalities, and the difficulties delivering the traditional cyber risk analysis when not working as a cyber security professional. Based on this information, next six (6) controls are set to evaluate the functionality of the planned model (Table 6):

Table 6, Monitoring criteria

Control one (1):	• The number of critical risks
Control two (2):	• Risk sources compared to elements of the method
Control three (3):	• Risk realization in the areas of the elements
Control four (4):	• The risks realized outside of the elements
Control five (5):	• Satisfaction of the employees using the method
Control six (6):	• Use of the method monthly / annually

7.10 Evaluation of the developed method

Two evaluation workshops (four (4), five (5)) were used for checking validity and relevance of developed method for pharmaceutical service cybersecurity risk management in hospital pharmacy environment. The goal for the first evaluation workshop was to get feedback from the ICT expert on how the presented model would be experienced regarding ICT office duties for hospital pharmacy and to identify potential defections with the model. The second evaluation workshop was arranged between the pharmacy personnel, Senior ICT expert and the author. The goal with second evaluation was to have feedback concurrently both from the pharmacy personnel and ICT experts how the developed method corresponds with their opinion of practical cybersecurity risk management tool and whether there are some misconceptions with the method.

7.10.1 Workshop four (4)

Workshop four (4) was held on 20th of July 2023 in case organization premises between Senior ICT Service Manager and the researcher. In this workshop, the Senior ICT Service Manager analyzed the developed pharmaceutical service cyber risk management model, elements, checklists, process, and monitoring criteria and model's validity and relevance from the information management office and service perspective. Participant was invited to the workshop by mutual invitation. Participation was based on their voluntary to contribute time and knowledge for this study. The workshop was kept in good spirit with an open-minded and objective attitude. The researcher reminded participant that all the results will be handled without any personal information.

Observations from workshop four (4) indicate the model's suitability for cybersecurity risk management purposes in ICT service meetings between information management office and pharmacy in case organization. The model was experienced versatile and easy to use with adequate checklists for frequent analysis of present situation. No changes were suggested to the method.

7.10.2 Workshop five (5)

Workshop four was held on 26th of July 2023 in the hospital pharmacy premises with the pharmacists (two invited), Senior ICT expert and the researcher. All participants were invited using email calendar invitation with subject and target for the workshop. In this workshop, the method was presented to the pharmacists and to the Senior ICT Expert. The researcher reminded participant that all the results will be handled without any personal information. The workshop was kept in good spirit with an open-minded and objective attitude. Participation was based on their voluntary to contribute time and knowledge for this study.

Participants analyzed the developed pharmaceutical service cyber risk management model, elements, checklists, process, and monitoring criteria and model's validity and relevance for hospital pharmacy operation. The author presented the method using Microsoft PowerPoint presentation and reminded of the original target and goal of the study. The participants discoursed of the number of required risk assessment rounds for maintaining checklists in appropriable level annually and presented their opinions of it. The Senior ICT Expert denoted the need for using the method in the service meetings with hospital pharmacy personnel and expressed, that cyber security persons should be involved in service meetings.

Observations from workshop five (5) express the model’s suitability for controlling cyber security risks of pharmaceutical services in hospital pharmacy operations. The model was experienced versatile and easy to use but requires work to preserve checklists up-to-date. The organization must determine the frequency of the cyber risk assessments for pharmaceutical services to maintain functionality of the method. As a result of the workshop, the method was accepted by the participants.

8 Results and findings

The findings of the study demonstrate conformity with the findings from the earlier studies used as references. The main finding was identifying the challenges with existing cyber security and risk management standards and frameworks considering their functionality as guidelines to hospital pharmacy daily operation. According to Duncan and Whittington (2014) there is not one standard or framework which could solve cyber security challenges for all businesses. Considerable amount of cyber security frameworks, standards and best practices are published to help organizations to manage and their cyber security risk management, but it is not clear which one to use in their own environment (Al-Ahmad and Mohammad, 2013). Businesses are different and those all face various threats in their operations. Each business should focus on analyzing their threat vectors, vulnerabilities and risks evolving from the operations (Taherdoost, 2022).

8.1 The target

Pharmaceutical services are a fundamental part of patient care and safety. Pharmacy operations are increasingly using information technology and new threats and risks emerge along with modern technology and changes in operations. Cyber security risk management needed to be improved to meet the organization’s responsibilities and requirements. Considering this, the aim of the study became relevant. The target was to implement method and principles to the hospital pharmacy on how to recognize threats and risks in their normal daily operations. To accomplish this target, research process was planned to deliver considerable amount of information covering pharmaceutical service operations in hospital pharmacy, employees’ abilities and orientation toward cyber security risk management, ICT senior experts understanding for cyber security risks and ICT environment, frameworks and standards for cyber risk management and earlier studies related to pharmaceutical services and supply chain management in the hospital pharmacy.

8.2 Data

A few standards and frameworks were included (chapter 5.5) to gather information on how those could be used in case organization to achieve a consistent cyber risk management model for hospital pharmacy. The finding was, that examined standards or frameworks could be considered for comprehensive cyber risk management in the organization but not only for hospital pharmacy purposes described for this study, because those do not introduce tools for pharmacy personnel for recognizing cyber security risks. Instead, presented frameworks and standards offer tools for the cyber security personnel and ICT personnel to use for the risk management duties and for comprehensive organization level cyber security risk management.

Chapter six (6) collects the information retrieved from current state analysis, questionnaire, workshops, and interviews. Chapter seven (7), "Designing the risk management model", associates the findings from the collected data between various sources. These findings represent valuable data which was used for creating the method for cyber risk management.

8.2.1 Data analyzing methods

The collected data were analyzed using classification and data triangulation methods. The classification was used with the results of the questionnaire and data triangulation with the data collected from interviews, workshops, and literature to answer the presented research question. Transcriptions of delivered interviews and workshops were used for accuracy. Transcriptions were done using standard language due to the professional field of participated persons were working for.

Triangulation method can be used to control quality of collected data by examining existing phenomena using multiple aspects (Kananen, 2014, 124). Without using triangulation method, the results of the examined phenomena could be more unilateral and might not be as comprehensive as with using triangulation. Classification was used to categorize received outcomes from questionnaire to understand, "How do the hospital pharmacy personnel understand and experience cyber security risks in their daily operations?".

8.3 Results

As a result of the study corresponding to the research question, the method (Figure 9), checklist (Table 5), process (Figure 10), and monitoring criteria for pharmaceutical service cyber risk management was created using the findings from the delivered questionnaire, workshops, interviews, and literature. The model includes eight (8) elements to control with screening items created into checklists. The screening items are changing according to risk assessment result, set goals for risk management and changing operational environment including legislation.

8.4 Validity and relevancy

The goal was to produce principles for pharmacy personnel, how to recognize threats and risks in their normal daily operations delivering pharmaceutical services. With the developed method, organization can improve their abilities to manage and control cyber security risks evolving from pharmaceutical service operations. Accordingly, same method can be used in other hospital pharmacies in Finland for similar purposes, and it can be integrated with cyber security management system used for comprehensive cyber security management in the organization. By changing elements and checklists according to each organization's own risk assessment results, the method can be used for multiple risk management purposes.

Results of the study were examined by case organizations' information management office experts responsible for ICT services to pharmacy and the pharmacy personnel responsible for risk management and pharmacy operations. Multiple evaluation rounds were done between received results from the workshops and interviews to ensure quality and authenticity of the results. The developed method and the elements in it are results of delivered research and are introduced in the study. According to Kananen (2014, 136), qualitative research must be based on results of the findings regardless of the authors thoughts.

8.5 Reliability

Results are based on research work including examination of current state of case organization, professional literature, implemented questionnaire, interviews and workshops, and designing of the cyber security management method, which all are introduced as part of the study. All the findings are presented and connected to the research topic and the result of the study. The study followed the planned research process and both research approach and methods were rationalized.

8.6 Ethicality

Within the delivered study, research methods, processes, collected data and results are described. References and citations are used according to APA 7 instructions and JAMK University of Applied Sciences’ Ethical Principles (2018) to avoid plagiarism. Personal information was not collected from the participants and participation was voluntary based on their will to contribute time and information to this research. Compensations were not given to any participants, and their consent was asked before engaging in any activities of the research. Research work in case organization was delivered in accordance with research permit agreement and results of the work were reported to the organization.

The goal of this work was to produce principles for hospital pharmacy for recognizing threats and risks in their daily operation delivering pharmaceutical services, which from the ethical perspective can be seen as indirect method to improve patient safety and security.

9 Conclusions

The study produced a method for the pharmaceutical services’ cyber security risk management in hospital pharmacy of the case organization. The method was developed based on the business need to recognize cyber security risks originating from the pharmaceutical service digital supply chain as discussed in chapter 1.3, Target and goal of the research. The developed method connects case organization’s internal policies, currently existing legislation, business need for improving cyber security risk procedures and the goal to produce principles to pharmacy personnel, how to recognize threats and risks in their normal daily operations.

Chapter two (2) describes the research approach models and reasons for the design research approach with qualitative methods. The target was to achieve change within cyber security management procedures with the limited amount of intervention by the author. According to Kananen (2013, 24), the change is a key factor in design research model whereas in action research, the researcher has a more active role with the development and intervention (Kananen, 2013, 29).

The research's structure was divided into five (5) sections described in chapter two (2). Research was conducted according to the chosen research approach and process including status analysis, data collection and analysis, development of the proposed method, intervention for feedback and conclusion of the research.

Data was collected using multiple methods including articles, standards, frameworks, other professional literature, and publications. Questionnaire was conducted for the case organization pharmacy employees and workshops and interviews were organized for both pharmacy and ICT personnel including internal and external experts.

The main research question was “What kind of method could be used to recognize and manage cyber security risks emerging from the pharmaceutical services supply chain in hospital pharmacy operations?” The developed method for managing cyber security risks within pharmaceutical service operations correlates with the primary research question. The method integrates with the organization comprehensive risk management model and improves cyber security risk management procedures related to pharmaceutical services. It offers tools for the pharmacy personnel to consider changes within the areas of main elements in the presented model which can compromise cyber security. Checklists encompassing screening items for main elements are to be used for controlling the risks and threats derived from the comprehensive cyber risk analysis. Risk analysis is proposed to include in the organization's annual plan for continuity of cyber security risk management.

For the supportive research question, "How can we achieve a consistent cyber risk management model for hospital pharmacy promoting risk management and cyber security management frameworks and standards?", the study addressed challenges with the frameworks and standards included in this research which do not introduce simple tools for people not dedicated in cyber security or information technology. The standards can be used for comprehensive cyber security management model and frameworks can be implemented correspondingly but require expertise. This study was limited view to pharmaceutical services in a hospital pharmacy and with this limitation, the consequence is valid for not implementing any of the examined frameworks or standards purely on these purposes.

Another supportive research question was, "How do the hospital pharmacy personnel understand and experience cyber security risks in their daily operations?". The questionnaire was conducted for hospital pharmacy personnel to collect information for this research question. The questionnaire was sent to 75 employees of which 16 employees, 21 %, returned the questionnaire with answers, which must be notified when analyzing the results. The collected answers represent the participants' own sentiments of each question and are valid in this perspective. The number of answers is low compared to the number of personnel invited to participate and decreases the credibility of the results gathered from the questionnaire.

10 Discussions

Recognizing and understanding the vulnerabilities, threats and risks in your business is crucial in today's all time changing environment to be able to deliver continuous business operations. In this way we manage to design and evaluate needed countermeasures or safeguards against unwanted situations and increase our resilience. The study focused on recognizing cyber security risks originating from the pharmaceutical services including supply chain structures in hospital pharmacy operations and implementing method to case organization to recognize and control cyber security risks as part of their daily function. Digitalization has a significant role in current pharmaceutical services and risks are changing along with digitalization and new services. Pharmaceutical services supply chain overall is designed to deliver lawful medicines to its clients (Brechtelsbauer et al., 2016). Integrating new technology with pharmaceutical supply chain transforms the risk matrix of the traditional supply chain structure and cyber security risks must be considered for integrity, availability, and continuity of the services (Boyens et al., 2021).

The research was based on the actual development need for cyber security risk management on pharmaceutical service supply chain digital operations in hospital pharmacy. The existing model of cyber security risk management had to be improved according to the business and the constantly evolving threat matrix. It was identified that there was a gap between cyber operations and the pharmaceutical service supply chain digital operations, and this thesis work was targeted to revise missing elements for pharmaceutical service cyber risk management. The challenge was that business could not recognize the lacking elements, and this must be studied before remodeling the cyber security risk management procedures to allocate the countermeasures competently.

The study represented a limited view to cyber security risk management in a definite environment. It did not cover all available standards or frameworks and reflects the sentiments of the case organization for having simplified principles for pharmaceutical service cyber security risk management in hospital pharmacy. The limitations used with the standards and frameworks can be seen as a weakness of this study along with the small number of participants answering the questionnaire. This stated the study addressed the elements for cyber risk sources to be observed within the daily operation and the process to maintain the consistency with the elements and key controls for the elements. Key controls for the elements depend on the risk assessment results and must be aligned with each organization's own business goals (Taherdoost, 2022).

Comparing the achieved results against the given research challenge, the result corresponds to the original research topic and questions. The author conducted the study according to the plan and tried to be impartial towards any information collected or observed. The aim was to develop a method and principles for cyber security risk management of pharmaceutical services understanding the operational environment and business need. The study accomplished a distinct method for pharmaceutical service cyber risk management in hospital pharmacy. This does not eliminate the need for a comprehensive cyber security management system in the organization rather than support its implementation in the case organization.

Criticism might be expressed towards literature search methods and limitations with used standards and frameworks. It is true, that with used search methods huge amount of usable information might be not found and more systematic method would help to find more accurate sources. The presented research questions were composed in early stage of the study and thinking retrospectively, the question related to existing frameworks and standards could have been more definite.

Future research could focus more deeply on cyber supply chain risk management discussed in chapter 5.3, Cyber security supply chain risk management. Boyens et al. (2021) publication expresses the key functions that many companies and organizations could benefit from as guidance for continuous C-SCRM program. But are businesses aware of C-SCRM programs and are they implementing, or have they implemented this program and what kind of benefits could be achieved when implementing this program properly?

This study was a limited review of pharmaceutical service cyber risk management method for hospital pharmacy in one organization. The case organization indicates that this method can be used in many ways, and it benefits the organization’s cyber security risk management overall. The study expresses that cyber security standards and frameworks should be used for implementing comprehensive cyber risk management and does not underrate their value in any meaning. The results of this study can be seen as targeted implementation of cyber risk management practices for assigned field of business operations and needs.

References

Act on Information Management in Public Administration 906/2019. https://www.finlex.fi/en/laki/kaannokset/2019/en20190906.pdf

Adebukola, A. A., Navya, A. N., Jordan, F. J., Jenifer, N. J., & Begley, R. D. (2022). Cyber Security as a Threat to Health Care. Journal of Technology and Systems, 4(1), 32–64. https://doi.org/10.47941/jts.1149

Al-Ahmad, W., & Mohammad, B. (2013). Addressing information security risks by adopting standards. *International Journal of Information Security Science*, *2*(2), 28-43.

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J., O'Leary, C., Eshaya-Chauvin, B., & Flahault, A. (2020). Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making, 20(1)*. https://doi.org/10.1186/s12911-020-01161-7

Bhuyan, S.S., Kabir, U., Escarano, J.M., Ector, K., Palakodeti, S., Wyant, D., Kumar, S., Levy, M., Kedia, S., Dasgupta, D., & Dobalian, A. (2020). Transforming Healthcare Cybersecurity from Reactive to Proactive: Current Status and Future Recommendations. J Med Syst 44, 98. https://doi.org/10.1007/s10916-019-1507-y

Boyens, J., Paulsen, C., Bartol, N., Winkler, K. and Gimbi, J. (2021), Key Practices in Cyber Supply Chain Risk Management: Observations from Industry, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8276

Brechtelsbauer, E., Pennell, B. T., Durham, M., Hertig, J. B., & Weber, R. J. (2016). Review of the 2015 Drug Supply Chain Security Act. *Hospital Pharmacy, 51(6), 493–500*. https://doi.org/10.1310/hpj5106-493

Caralli, R., Stevens, J. F., Young, L. R., & Wilson, W. R. (2018). Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process (Version 1). Carnegie Mellon University. https://doi.org/10.1184/R1/6574790.v

Conti cyber attack on the HSE. (2021). *https://www.hse.ie/eng/services/publications/*. Retrieved Feb 2, 2023, from https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas, 113, 48–52. https://doi.org/10.1016/j.maturitas.2018.04.008

Cybersecurity, C. I. (2018). Framework for improving critical infrastructure cybersecurity. *URL: https://nvlpubs. nist. gov/nistpubs/CSWP/NIST. CSWP, 4162018*. https://doi.org/10.6028/NIST.CSWP.04162018

Data Protection Act 1050/2018. Issued in Helsinki on 5 December 2018. https://www.finlex.fi/en/laki/kaannokset/2018/en20181050

Digital Pool (2020a). *Johdon ohjaus on ratkaisevaa yrityksen kyberkestävyyden kannalta*. https://www.digipooli.fi/fi/ajankohtaista/uutinen/johdon-ohjaus-ratkaisevaa-yrityksen-kyberkestavyyden-kannalta

Digital Pool (2020b). *Current State of Cybersecurity in Different Sectors – Key Survey Findings.* https://www.digipooli.fi/sites/digipooli/files/2021-06/The-current-state-of-cybersecurity-in-different-sectors_2020.pdf

Duncan, B., & Whittington, M. (2014). Compliance with standards, assurance and audit: does this equal security?. In *Proceedings of the 7th International Conference on Security of Information and Networks* (pp. 77-84). http://dx.doi.org/10.1145/2659651.2659711

European union, Charter of Fundamental Rights of the European Union. (2012). *Official Journal C 326/2, 24.10.2012, 391. Article 7*. Retrieved from eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C:2012:326:FULL

European Union Agency for Cybersecurity, (2016). *Smart hospitals: security and resilience for smart health service and infrastructures*, *European Network and Information Security Agency.* https://data.europa.eu/doi/10.2824/28801

Fimea (2023). *Medical devices.* Retrieved from https://www.fimea.fi/web/en/medical-devices

Fimea (2023). *Pharmaceutical industry*. Retrieved from https://www.fimea.fi/web/en/supervision/pharmaceutical_industry

Fimea (2023). *Sairaala-apteekit ja lääketietokeskukset*. Retrieved from https://www.fimea.fi/apteekit/sairaala-apteekit_ja_laakekeskukset

FORCE, J. T. (2018). Risk Management Framework for Information Systems and Organizations. *NIST Special Publication*, *800*, 37. *URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf*. https://doi.org/10.6028/NIST.SP.800-37r2

Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., & Linkov, I. (2020). Multicriteria decision framework for cybersecurity risk assessment and management. *Risk Analysis*, *40*(1), 183-199. Https://doi.org/10.1111/risa.12891

Gioulekas, F., Stamatiadis, E., Tzikas, A., Gounaris, K., Georgiadou, A., Michalitsi-Psarrou, A., Doukas, G., Kontoulis, M., Nikoloudakis, Y., Marin, S., Cabecinha, R., & Ntanos, C. (2022). A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures. Healthcare (Basel, Switzerland), 10(2), 327. https://doi.org/10.3390/healthcare10020327

Health Care Act 1326/2010. Issued in Helsinki on 30 December 2010. https://www.finlex.fi/en/laki/kaannokset/2010/en20101326

ISO/IEC 27001:2022. (2022). *Information security, cybersecurity and privacy protection - Information security management systems - Requirements.* Retrieved from https://www.iso.org/standard/27001

ISO/IEC 31000:2018. (2018). *Risk management – Guidelines*. Retrieved from https://www.iso.org/standard/65694.html

JAMK University of Applied Sciences. (2018). *Ethical Principles*. Retrieved from https://www.jamk.fi/en/media/34826

Kananen, J. (2013). *Design Research (applied action research) as thesis research: A practical guide for thesis research*. Jyväskylän ammattikorkeakoulu.

Kananen, J. (2014). *Toimintatutkimus kehittämistutkimuksen muotona. Miten kirjoitan toimintatutkimuksen opinnäytetyönä?* Jyväskylän ammattikorkeakoulu

Lehto M., Pöyhönen J., & Lehto M. (2019). Kyberturvallisuus sosiaali- ja terveydenhuollossa. http://urn.fi/URN:ISBN:978-951-39-7711-5

Lääketeollisuus. (n. d.). *Lääkkeiden jakelu*. Retrieved 8.8.2023 from https://www.laaketeollisuus.fi/tietoa-laakkeista/laakkeiden-jakelu.html

Mattioli, R., Malatras, A., Hunter, E.N., Penso, M.G.B., Bertram, D., Neubert, I., (2023). *Identifying emerging cybersecurity threats and challenges for 2030,* European Union Agency for Cybersecurity. https://data.europa.eu/doi/10.2824/117542

Muthuppalaniappan, M., & Stevenson, K. (2021). Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health. *International Journal for Quality in Health Care, 33(1).* https://doi.org/10.1093/intqhc/mzaa117

Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors*, *21*(15), 5119. https://doi.org/10.3390/s21155119

Pharma Industry Finland. (n. d.). *Distribution of pharmaceuticals*. Retrieved 7.7.2023 from https://www.pif.fi/medicines/distribution-of-pharmaceuticals.html

Pharma Industry Finland. (n. d.). *Medicines verification system.* Retrieved 7.7.2023 from https://www.pif.fi/responsibility/medicines-verification-system

Solfa, F. D. G. (2022). Impacts of Cyber Security and Supply Chain Risk on Digital Operations: Evidence from the Pharmaceutical Industry. *International Journal of Technology, Innovation and Management (IJTIM), 2(2), 18–32.* https://doi.org/10.54489/ijtim.v2i2.98

Taherdoost, H. (2022). Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. *Electronics, 11(14), 2181*. https://doi.org/10.3390/electronics11142181

The Constitution of Finland 731/1999. https://finlex.fi/en/laki/kaannokset/1999/en19990731.pdf

The Ministry of Finance. *Areas of expertise*. Retrieved from https://vm.fi/en/areas-of-expertise

The Ministry of Finance. *Digitalization*. Retrieved from https://vm.fi/en/digitalisation

The Ministry of Finance. *Duties and other activities.* Retrieved from https://vm.fi/en/duties-and-other-activities

The Ministry of Finance. *Ministry.* Retrieved from https://vm.fi/en/ministry

The Ministry of Finance. *Projects and legislation.* Retrieved from https://vm.fi/en/ministerial-working-group-on-developing-the-digital-transformation-the-data-economy-and-public-administration

The Ministry of Finance. *Public Sector ICT*. Retrieved from https://vm.fi/en/public-sector-ict

The Ministry of Finance. *Reform.* Retrieved from https://vm.fi/en/health-social-services-reform

The National Cyber Security Centre (2022). *Information security and data protection requirements for social welfare and healthcare procurements.* Retrieved from https://www.kyberturvallisuuskeskus.fi/en/ncsc-news/instructions-and-guides/information-security-and-data-protection-requirements-social

The National Cyber Security Centre (2023). *Deployment of Cybermeter in social welfare and healthcare organizations.* Retrieved from https://www.kyberturvallisuuskeskus.fi/en/ncsc-news/instructions-and-guides/deployment-cybermeter-social-welfare-and-healthcare-organisations

Appendices

Appendix 1. Questionnaire (in Finnish)

Arvoisa vastaanottaja

Pyyntö osallistua opinnäytetyöhön

Sinua pyydetään osallistumaan opinnäytetyöhön, jossa tutkitaan, millaisilla menetelmillä kyberturvallisuuden riskejä voisi hallita lääkehuollon osalta kohdentuen sairaala-apteekin toimintaan. Opinnäyte työ tehdään [redacted] sairaala-apteekkiin ja työn tekijänä toimii Jari Liesoja. Opinnäytetyö on osa Jyväskylän ammattikorkeakoulun kyberturvallisuuden YAMK tutkinto-ohjelmaa. Vastaaminen kyselyyn kestää arviolta noin 5–15 minuuttia.

Vapaaehtoisuus ja suostumus tietojen hyödyntämiseen

Opinnäytetyöhön osallistuminen on täysin vapaaehtoista ja voit keskeyttää osallistumisen koska tahansa. Opinnäytetyöstä kieltäytyminen tai sen keskeyttäminen ei vaikuta millään tavalla kohteluusi. Osallistumalla Sinulle tarjottuun kyselyyn annat samalla suostumuksesi osallistua opinnäytetyöhön ja vastausten hyödyntämiseen osana tutkimuksen aineistoa.

Opinnäytetyön tarkoitus

Tämän opinnäytetyön tarkoituksena on löytää tarkoitukseen sopivia keinoja kyberturvallisuuden riskien hallinnan ja tunnistamisen osalta, joita voidaan hyödyntää sairaala-apteekin yleisissä työtehtävissä. Kyberturvallisuuden kautta esiintyvät riskit ja niiden hallinta poikkeaa yksikön normaaleista työtehtävistä, joten hallintakeinojen tulee olla selkeitä ja tarkoitukseen sopivia. Kyberturvallisuuden riskit tässä opinnäytetyössä kohdentuvat digitaalisen toimitusketjun kautta muodostuviin riskeihin. Opinnäytetyö ei ota kantaa yksikön muihin riskilajeihin tai potilasturvallisuuteen suorasti.

Tietojen luottamuksellisuus, säilytys ja tietosuoja

Tutkimuksessa ei kerätä henkilötietoja. Tutkimusaineistosta ei pystytä päättelemään vastaajan henkilöllisyyttä, eikä annettuja vastauksia voida yhdistää tiettyyn luonnolliseen henkilöön. Tutkimusaineisto on tarkoitettu vain tutkijan käyttöön, eikä sitä jaeta tutkimuksen ulkopuolisille henkilöille.

Lisätiedot

Pyydän Sinua tarvittaessa esittämään tutkimukseen liittyviä kysymyksiä opinnäytetyön tekijälle.

Nimi: Jari Liesoja
Puh.: +358[redacted]
S-posti: [redacted]

Avoimet kysymykset:

Ohje: Vastaa lyhyesti oman tehtäväsi näkökulmasta ja oman ymmärryksesi ja tietämyksesi mukaan kysymyksiin.

1. Kuuluuko kyberturvallisuuden riskien ymmärtäminen ja uhkiin reagoiminen mielestäsi Sinulle työtehtäviisi liittyen?
2. Onko Sinulla riittävästi mahdollisuuksia tai osaamista tällä hetkellä kyberturvallisuuden riskien tunnistamiseen?
3. Millaisia kyberturvallisuuden riskejä näet oman työsi kautta lääkehuollon digitaaliseen toimitusketjuun liittyen?
4. Millä tavoin lääkehuollon digitaaliseen toimintaketjuun kohdistuva kyberhyökkäys voisi vaikuttaa oman organisaatiosi toimintakykyyn?
5. Millaisilla menetelmillä kyberturvallisuuden riskejä mielestäsi voisi tunnistaa ja hallita omaan työhösi liittyen nykytilaa paremmin?
6. Tarvitsetko lisää koulutusta kyberturvallisuuden uhkien tunnistamiseksi ja ymmärtämiseksi?

Suljetut kysymykset vastausvaihtoehtoineen:

Ohje: Voit valita kaikki asiaan mielestäsi liittyvät kohdat

1. Mitä seuraavista tunnistat liittyväksi kyberturvallisuuden riskienhallintaan lääkehuollon osalta:
   a. Tietoturva- ja tietosuojakoulutukset
   b. Säännölliset katselmoinnit tietojärjestelmien osalta
   c. Ajantasainen käyttöoikeuksien hallinta
   d. ICT-ympäristön kuvausten ajantasaisuus
   e. Tietojärjestelmätoimittajien etäyhteydet omiin tietojärjestelmiin
   f. Toimitusketjuun liittyvät tietojärjestelmät
   g. Toimittajien etäyhteydet ja pääsy organisaation järjestelmiin
   h. Internetin käyttö työpaikalla
   i. Sähköpostin käyttö työpaikalla
   j. Kyberturvallisuuden hallintajärjestelmä
   k. Organisaation tietoturva- ja tietosuojapolitiikka
   l. Sopimusten hallinta
   m. Hankintoihin liittyvät kyberturvallisuuden vaatimukset

2. Voisiko kyberturvallisuuden riskienhallintaa mielestäsi parantaa organisaatiossasi:
   a. Selkeyttämällä vastuita kyberturvallisuuden riskienhallinnan osalta
   b. Lisäämällä resursseja tieto- ja kyberturvallisuuden tehtävien hoitamiseen
   c. Muuttamalla hankintaprosessia uusien hankittavien järjestelmien osalta

   d. Lisäämällä toimittajayhteistyötä ja parantamalla toimittajien hallintaa
   e. Lisäämällä työntekijän vastuuta
   f. Lisäämällä johdon vastuuta
   g. Lisäämällä koulutusta työntekijöille kyberturvallisuuden riskienhallinnasta
   h. Tarjoamalla selkeitä ohjeita ja menetelmiä riskien tunnistamiseksi ja käsittelemiseksi
   i. Toteuttamalla säännöllisiä riskienkartoituksia yksikön toiminnassa

3. Voisiko tieto- ja kyberturvallisuustoimintamalleja parantaa organisaatiossasi
   a. Lisäämällä vastuuta tieto- ja kyberturvallisuushenkilöille
   b. Tarjoamalla selkeitä toimintamalleja tieto- ja kyberturvallisuuden riskien tunnistamiseen omassa toiminnassa
   c. Pitämällä yhteisiä koulutuksia tieto- ja kyberturvallisuuden riskien tunnistamisesta ja hallinnasta
   d. Hankkimalla uusia tietojärjestelmiä raportointia varten
   e. Tuottamalla organisaation intranettiin kattavasti ohjeistusta kyberturvallisuuden uhkien ja havaitsemisesta ja riskien käsittelystä
   f. Lisäämällä vastuuta kaikille työntekijöille
   g. Lisäämällä resursseja tieto- ja kyberturvallisuustoimintaan
   h. Ulkoistamalla tieto- ja kyberturvallisuustoiminnan