TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Kristiina Šamanina 210732IVSB

Securing Aesthetic Medicine Company Samleks OÜ by the ISO 27001 Standard

Bachelor's thesis

Supervisor: Valdo Praust
MSc

Tallinn 2023

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Kristiina Šamanina 210732IVSB

Esteetilise meditsiini ettevõtte Samleks OÜ kindlustamine ISO 27001 standardi järgi

Bakalaureusetöö

Juhendaja: Valdo Praust
MSc

Tallinn 2023

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Kristiina Šamanina

11.05.2023

Abstract

Information security has become increasingly important for individuals and businesses, especially in the medical industry, due to the rise of cyber threats. The ISO 27001 standard provides a systematic approach to managing information security risks, which can be adopted by businesses, including small aesthetic medicine companies. This study aims to assess the application of ISO 27001 in such companies by reviewing the standard's requirements, analysing potential benefits and challenges, and providing implementation guidelines and recommendations. The research focuses on information security challenges faced by small aesthetic medicine companies and proposes solutions to improve their practices. The study aims to answer research questions on the possibility of ISO 27001 implementation, key information security risks, common practices, and business owners' attitudes towards information security. The research findings can provide valuable insights into ISO 27001 adoption and improve information security practices in the industry.

This thesis is written in English and is 59 pages long, including 5 chapters and 2 tables.

List of abbreviations and terms

BCP	Business Continuity Plan
BS	British Standard
BSI Group	British Standards Institution Group
CAL	Cell-assisted lipotransfer
DTI	Department of Trade and Industry
IBM	International Business Machines Corporation
IEC	International Electrotechnical Commission
ID	Identification
ISMS	Information security management system
IoT	Internet of Things
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
OÜ	Osaühing (Private limited company in Estonia)
RTP	Risk Treatment Plan
SoA	Statement of Applicability
IT	Information Technology

Table of contents

List of tables

1 Introduction

In today's evolving environment, information security has become important for individuals and businesses. With the increasing use of technology and the internet, personal information can be vulnerable to cyber threats such as data breaches, hacking, and identity theft. In fact, the attacks on the medical industry have surged in 2022 according to IBM which makes it crucial to protect personal information from these risks and ensure its confidentiality.[1] Breaches can cause financial loss and reputational damage. It is important to note that even smaller businesses are a target, so it is important to secure them too.[2]

To secure sensitive data, businesses can adopt various standards and frameworks, such as the ISO 27001 standard. This standard provides a systematic approach to managing information security risks and is relevant in all industries, including the medical industry.

Demand for aesthetic medicine procedures and products has been rising rapidly.[3] Due to high demand, securing information regarding clients and companies is also important, especially for smaller businesses. Increased use of technology has to be taken into account since there is a need not only to secure sensitive information about clients but also to ensure the confidentiality of medical records. Its popularity has risen due to its minimally invasive nature and quick results. Compared to cosmetic surgeries, the recovery time, cost, and duration are relatively smaller. The risk of complications for aesthetic medicine procedures can be smaller but never non-existent considering that a person does need a medical license to be able to perform them.

1.1 Research Objectives

The objectives of this research are to review the main requirements of the ISO 27001 standard and assess its application to the medical industry, evaluate the current state of information security practices in the medical industry, analyse the potential benefits and challenges of implementing ISO 27001 in a medical company, develop a set of guidelines for implementing the ISO 27001 standard in a small aesthetic medicine company, and provide recommendations for its adoption in such businesses.

1.2 Scope and Limitations

The focus is on a small aesthetic medicine company and its challenges in securing its operations. It will analyze the current state of information security practices in the industry and propose solutions to improve them.

This research will not include any other ISO standards, and the impact of external factors such as competition will not be considered.

1.3 Research problem

Despite the growing significance of information security in the aesthetic medicine sector, more research is required to understand how to implement ISO 27001 in small aesthetic medicine businesses. This is because there hasn't been much work done to secure these medically related small businesses.

1.4 Research questions

This research aims to answer the following questions:

1. What is the general possibility of implementing iso 27001 in aesthetic medicine companies?
2. What are the key information security risks faced by small medical aesthetics businesses, and how can they be effectively mitigated?
3. What are the attitudes of medical aesthetics business owners towards information security, and what factors influence their adoption of best practices?

2 Background

This chapter provides a comprehensive overview of the aesthetic medicine industry and the ISO 27001 standard. It also discusses what ISO 27001 controls suit a small company with minimal infrastructure such as Samleks OÜ.

The aesthetic medicine industry has experienced rapid growth and popularity in recent years, as people seek minimally invasive procedures and quick results. However, the use of technology and personal data also poses potential risks for clients and companies themselves. Personal information can be vulnerable to cyber threats, leading to data breaches or cyber-attacks that can have a significant impact on individuals and businesses. In this context, information security management systems (ISMS) have become increasingly important in ensuring the confidentiality, integrity, and availability of information.

The ISO 27001 standard is a globally recognized framework that provides guidelines for establishing and maintaining an ISMS. Understanding the background of the aesthetic medicine industry and the ISO 27001 standard is essential for exploring their relevance and implications for information security.

2.1 Overview of the aesthetic medicine industry

Aesthetic medicine is art and science combined into one and is an emerging branch of medicine. Its purpose is to enhance appearance by using various procedures and techniques. The target of this medical branch is to improve the looks, texture, and contours of the skin all over the body. There are also aesthetic surgeries that sometimes overlap with aesthetic medicine, the main difference is that surgeries are extremely invasive compared to aesthetic medicine where the focus lies more on employing techniques and technologies. Those technologies are often minimally invasive and are done without general anaesthesia. There are specific procedures that remain exclusively in aesthetic surgery and they are the following: underminings, dissection, or skin excisions, such as rhytidectomy, brachioplasty, and abdominoplasty. These procedures should be done only in the hospital setting and with general anaesthesia. What is considered invasive in aesthetic medicine are dermal or subcutaneous injections, punctures, or small incisions. For example, botulinum toxins, temporary fillers, fat transfer, suture lifts, and various forms of lip-otoplasty. [4]

The aesthetic medicine branch is experiencing rapid growth in its demand due to patients' demand for non-invasive procedures. The procedures are not done for health reasons but rather for enhancing the outer appearance. Patients like this are unique to this specific medical branch since usually, most specialists focus diagnosis and treatment of pathologies and illnesses. Thanks to the availability of non-surgical procedures such as botulinum toxins, hyaluronic acid fillers, and others, patients can now quickly and discreetly improve their appearance and feel better without significant downtime.[4]

The attraction towards procedures like this is natural since they offer almost immediate natural-looking results without restricting everyday activities. However, aesthetic surgeries cannot be replaced by such procedures. From time to time less invasive procedures and techniques are preferred instead of surgery to get a similar effect on the appearance.[4]

The aesthetic medicine that is known today has evolved from various inventions and discoveries that come from specialists with different medical backgrounds. One such practitioner was Jean Carruthers, who was an ophthalmologist. He discovered that using botulinum toxin can have a remarkable result on the appearance which is the most performed procedure since. A dermatologist Jeffrey Klein invented tumescent anaesthesia, allowing lipoplasty to be performed in an office-based setting without any sedation or general anaesthesia. Numerous gynecologists like Fischer, Ilouz, and Fournier have also contributed to the industry in the 1980s with plastic, general surgeries, and liposuction. Fillers were already in use for quite some time, what really helped to revolutionize the use, was the development and approval of safe, cross-linked hyaluronic acid fillers. Thanks to that there were remarkable improvements in the practices of soft tissue augmentation for treating wrinkles and contouring the face and body. After that, the following breakthrough would be laser treatment. In 1983 the development of laser medicine and dermatology emerged after the initial proposal of selective photo-thermolysis by Anderson and Parrish. The next popular trend, already in the 1990s was carbon dioxide laser skin resurfacing. Nowadays it has been mostly replaced by safer devices. Another significant improvement to the dissemination of knowledge on the aesthetic applications of lasers and lights was made by numerous dermatologists, one of them was Goldberg. Numerous books on topics like liposuction, facial rejuvenation, and body contouring were made by a general cosmetic and oncologist surgeon Shiffmann. Therefore, this medical branch is characterized by a collection of different techniques that are developed from several other medical disciplines: dermatology, plastic, reconstructive surgery, laser medicine, and many others.[4]

Procedures that aesthetic medicine offers, target mostly the aging signs of the body and face which include abnormal skin pigmentation, skin laxity, ptosis, rhytids, fat loss, and contour irregularities such as tear trough deformity. A summary of the most common procedures can be seen below in Table 1. [4]

Table 1 Procedures in aesthetic medicine [4]

Indication	**Treatment modality**	**Example products/devices**
Hyperdynamic rhytids	Chemodenervation	Botox, Dysport, Xeomin
Lower face rhytids	STA with fillers	Restylane, Teosyal global action, Juvederm
Facial contouring	STA with fillers, fat	SubQ, Teosyal ultimate, Radiesse
Photoaging	Skin resurfacing	Fractional CO, lasers, chemical peels
Acne scarring	Micro-needling	Genuine dermaroller
Textural irregularities	Microdermabrasion	SilkPeel

Indication	Treatment modality	Example products/devices
Telangiectasias, varicose veins	Sclerotherapy	Fibro-vein, sclerofoam
Ptosis jowls, brow, cheeks, neck	Suture lifting techniques	Silhouette sutures, Anchorage sutures
Dyschromias	Selective photothermolysis	Intense pulsed light
Skin laxity	Radiofrequency, infrared	Kontur MD, titan
Breast augmentation	STA with fillers	Macrolane VRF 20/30
Lipoplasty	Ultrasound-assisted lipoplasty	VASER
Striae	Carboxytherapy	Carboxypen, RioBlush

Numerous aesthetic medicine procedures such as mesotherapy, lipoplasty, and chemodenervation with botulinum toxins have been carried out for several decades. In recent years aesthetic medicine has integrated established techniques with newer ones. For example, hyaluronic acid fillers, skin tightening, fractional resurfacing, third-generation ultrasound-assisted lipoplasty, and advanced skin imaging. To implement techniques safely, specialists must have proper theoretical and practical training in anatomy, aging, patient assessment and selection, anesthesia, technique, probable side effects, complications, and their management. A thorough knowledge of the materials, products, and devices in use should be attained in order to provide safe procedures. There are worldwide credible training programs that provide instruction and firsthand training for physicians and surgeons with different levels of experience. [4]

The most remarkable breakthrough in aesthetic medicine was the usage of botulinum toxin type A. It is used for one of the aging signs of the skin, wrinkles, and it remains the most widely performed procedure even now. The future of botulinum toxins includes the emergence of new brands and further advancement in the already existing techniques for providing better results. A central role for aesthetic medicine will still fall onto facial rejuvenation and restoration of volume. New approaches Cell-assisted lipotransfer (CAL) and stem cell-enriched fat transfer are being developed for battling the problem of graft cell survival after grafting to the face or other body parts.[4]

In the future, an important role falls on lasers, ultrasound, and radiofrequency technologies. New technologies that are becoming more popular are fractional lasers, focused ultrasound devices, and multipolar radiofrequency technology, which are used for fat reduction and skin tightening.[4]

Today, one of the fastest-growing medical fields is antiaging medicine. Because of this, aesthetic medicine became so widely practiced and demanded. [4]

In conclusion, the demand for anti-aging procedures is growing rapidly, which makes this industry widely spread and practiced. There are surgical and non-invasive procedures in this industry, and new techniques are constantly emerging. The use of botulinum toxin was a breakthrough for treating aging signs such as wrinkles. In the future, laser treatments might become the next emerging trend. [4]

2.2 Overview of ISO 27001 standard

ISO 27001 is an international standard developed for managing information security. The original publication of the standard happened in 2005 [5] together with International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), and then it was revised again in 2013 and 2022. [6][7] There exist many variants of this standard that are nationally recognized. Standard has detailed requirements for acquiring, implementing, and improving an ISMS. The aim of the information security management system is to help organizations secure their valuable assets. In case organizations meet the requirements, they can get certified after completing the audit successfully. The effectiveness of such a process and the standard itself has been covered in a large-scale study that was conducted in 2020.[8] Further, the standard history certification and how it works will be discussed.

The standard BS 7799 was originally published in 1995 by the BSI Group [9]. It consisted of several parts that were written by the UK government's Department of Trade and Industry (DTI). In 1998, the part that contained best practices for information security management was revised and eventually adopted by ISO as ISO/IEC 17799, “Information Technology - Code of Practice for information security management." in 2000. It was jet again revised in June 2005 and then eventually incorporated into ISO 27000 family as ISO/IEC 27002 in July 2007. Altogether there were 3 parts published. The second part was named "Information Security Management Systems - Specification with guidance for use." with a focus on implementing ISMS and the third part was published already in 2005, which covered risk analysis and management. [10][11]

Most organizations already have multiple information security controls. Security controls are measures to avoid, detect, counteract, or lower security risks to assets such as information, computer system, and other valuable aspects of the company. In the information security field, these controls protect multiple aspects: confidentiality, integrity, and availability of information. They can be referred to as frameworks or standards.[12]

The absence of ISMS makes controls fragmented, and they lack order. When the controls are used properly, each of them addresses specific aspects of information technology or data security specifically. They do leave anything that does not belong to previously mentioned categories and leave other information assets such as paperwork and proprietary knowledge, less protected. Moreover, the management of business continuity planning and physical security may occur separately from IT or information security.[12]

The following parts are required by ISO/IEC 27001 from the management:

1. examine the state of organizational information security risks and take into consideration the threats, vulnerabilities, and impacts.

2. choose what controls can be applied to the company (considering the nature of the business, infrastructure, and size) or apply other risk treatment methods to address threats that are considered unacceptable.
3. Develop a management process that ensures the ISMS controls continue to meet the information security needs of the company and review them in case of major changes organization. For example, relocations, significant growth in staff and departments, etc. It is important that people who are responsible for managing ISMS can adapt the controls accordingly. [12]

The certification process involves testing the controls in ISO 27001, what controls exactly is dependent on who would be the auditor. It can be any control that has been implemented in the company (usually defined in the scope of ISMS), and the goal is to prove that it works effectively. The responsibility of defining the scope falls onto management, for example, they have decided to get ISO/IEC 27001 certification in a single location or unit. [13]

There are many more standards in ISO/IEC 27000 family, they provide additional help for certain aspects of developing an ISMS [14][15]. In order to be certified in ISO/IEC 27001, it involves a three-staged external audit process, the same as with other ISO standards. [16][17]

The three stages are the following:

Stage 1: this is a preliminary stage, it is to get a better overview of the organization and the key points that should be implemented, which are information security policy, Statement of Applicability (SoA), and Risk Treatment Plan (RTP).

Stage 2: now there will be more detailed testing of ISMS against the requirements that are specified in ISO/IEC 27001. The auditor must find evidence of how the company's implemented ISMS is working in the company as described in the documents provided. For example, confirming that points provided in RTP are implemented. The audits are usually performed by ISO/IEC 27001 Lead Auditors.

Stage 3: this is called the ongoing stage which involves follow-up reviews to confirm that ISMS is still working efficiently as it was during the certification stage. They should happen annually or more frequently depending on how mature the ISMS is in the organization. [18]

ISO 27001 standard can be implemented in numerous companies no matter the size or industry, even if it has a wide range of controls, it can still be applied to smaller companies. Not all of the controls have to be applied, only the ones that suit the business's needs, which makes it highly customizable.

2.2.1 ISO 27001 Controls and their applicability to Samleks OÜ

ISO/IEC 27001 contains 114 controls which are categorized into 14 groups and in those 14 groups, there are 35 categories in each, not all of them can be applied to this particular company as it has a simple infrastructure and minimal assets. The control groups are listed further:

- A.5: Information security policies
- A.6: Organization of information security
- A.7: Human resources security.
- A.8: Asset management
- A.9: Access control
- A.10: Cryptography
- A.11: Physical and environmental security
- A.12: Operations security
- A.13: Communications security
- A.14: System acquisition, development and maintenance
- A.15: Supplier relationships
- A.16: Information security incident management
- A.17: Information security aspects of business continuity management
- A.18: Compliance

To understand why certain controls from each group were more suitable for this company, it is important to grasp what each of them contains. Each of the 14 groups is explained briefly.**[19]**

1. **Information security policies:** This section consists of management direction for information security. It outlines the importance of providing management

direction and support for information security in line with business needs and legal requirements. The policies developed should address various requirements such as business strategy, regulations, legislation, contracts, and the information security threat environment. The information security policy should define information security, objectives, and principles to guide all activities relating to information security, assign responsibilities for information security management to defined roles, and establish processes for handling deviations and exceptions. In larger and more complex organizations, internal policies are particularly useful and should be reviewed periodically to ensure their continuing suitability, adequacy, and effectiveness, especially in the event of significant changes in the company structure.**[19]**

2. **Organization of information security:** This consists of these: internal organization, mobile devices and teleworking chapters.

   Internal organization chapter provides guidelines for establishing a management framework to initiate and control the implementation and operation of information security within an organization. It outlines the roles and responsibilities for information security, segregation of duties to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets, maintaining appropriate contacts with relevant authorities and special interest groups, and integrating information security into project management methods. These guidelines are aimed at reducing the risk of accidental or deliberate misuse of an organization's assets and ensuring that information security risks are identified and addressed in all projects.**[19]**

   Mobile devices and teleworking segment provide guidelines for ensuring the security of teleworking and the use of mobile devices. To manage the risks associated with mobile devices, it is essential to adopt a policy and support security measures. The mobile device policy should consider registration, physical protection, restriction of software installation, requirements for mobile device software versions and applying patches, restriction of connection to information services, access controls, cryptographic techniques, malware protection, remote disabling, erasure or lockout, backups, and usage of web services and web apps. Similarly, a policy and supporting security measures should be implemented for teleworking sites. The guidelines and arrangements should include the provision of suitable equipment, definition of the work permitted, hours of work, the classification of information that may be held, and access to internal systems and services that the teleworker is authorized to access. Other considerations include physical security, rules and guidance on family and visitor access to equipment and information, provision of hardware and software support, and suitable communication equipment, including methods for securing remote access.**[19]**

3. **Human resources security:** this control consists of the following parts: prior to employment, during employment, termination and change of employment.

   Prior to employment, the segment covers the importance of screening employees and contractors to ensure that they understand their responsibilities and are suitable for the roles they are being considered for. Background verification checks should be carried out in accordance with relevant laws, regulations, and ethics and should take into account all relevant privacy and employment-based legislation. These verification checks should include the availability of satisfactory character references, verification of academic and professional qualifications, independent identity verification, and more detailed verification such as credit review or criminal record review. Additionally, procedures should define criteria and limitations for verification reviews, and a screening process should also be ensured for contractors. The contractual agreements with employees and contractors should state their and the organization's responsibilities for information security. This includes obligations for employees or contractors to sign a confidentiality or non-disclosure agreement, legal responsibilities and rights, and responsibilities for the handling of information. Finally, information security roles and responsibilities should be communicated to job candidates during the pre-employment process, and a code of conduct may be used to state the employee's or contractor's information security responsibilities. **[19]**

During employment part outlines the measures necessary for organizations to ensure that employees and contractors fulfill their information security responsibilities. It recommends that management should require all employees and contractors to apply information security policies and procedures, including having them properly briefed on their information security roles and responsibilities prior to being granted access to confidential information or information systems. Additionally, employees should receive information security awareness, education, and training to raise their level of awareness and motivate them to comply with information security policies. An information security awareness programme should be established to make employees aware of their responsibilities and should be updated regularly to stay in line with organizational policies and procedures. Finally, a formal and communicated disciplinary process should be in place to take action against employees who have committed an information security breach. If employees are not made aware of their information security responsibilities, they can cause considerable damage to the organization. **[19]**

The termination and change of employment section provides guidance for protecting an organization's interests during the process of changing or terminating employment. The document suggests that information security responsibilities and duties that remain valid after termination or change of employment should be defined, communicated, and enforced. Communication of termination responsibilities should include ongoing information security requirements and legal responsibilities, and responsibilities contained within any confidentiality agreement and terms and conditions of employment should continue for a defined period after the end of employment. The document also highlights that changes of responsibility or employment should be managed as the termination of the current responsibility or employment combined with the initiation of the new responsibility or employment. The human resources function is responsible for the overall termination process and works together with the supervising manager to manage the information security aspects of relevant procedures. Communication of changes to personnel and operating arrangements may be necessary. **[19]**

4. **Asset management:** This category consists of these smaller chapters: responsibility for assets, information classification and media handling.

   Responsibility for assets section provides guidelines for protecting organizational assets associated with information and information processing facilities. This includes identifying and maintaining an accurate inventory of assets, assigning ownership to assets, establishing rules for acceptable use of assets, and ensuring the return of all organizational assets upon termination of employment or contract. It emphasizes the importance of asset management in risk management and also highlights the need for awareness among employees and external parties regarding information security requirements. Proper asset management is necessary for effective protection, as well as for other purposes such as health and safety, insurance, and financial reasons. The identified owner of assets may be an individual or entity with approved management responsibility for controlling the entire asset lifecycle, and they should be responsible for proper management of the asset over the entire lifecycle.**[19]**

   Information classification section of asset management is to ensure that information receives an appropriate level of protection in accordance with its importance to the organization. This involves classifying information based on legal requirements, value, criticality, and sensitivity to unauthorized disclosure or modification. The classification scheme should be consistent across the organization and owners of information assets should be accountable for their classification. Procedures for information labelling and handling assets should also be developed and implemented in accordance with the information classification scheme. The implementation of information classification provides people who deal with information with a concise indication of how to handle and protect it, which reduces the need for case-by-case risk assessment and custom design of controls. However, over-classification can lead to the implementation of unnecessary controls resulting in additional expense, while under-classification can endanger the achievement of business objectives. Organizations should also be aware that classified assets are easier to identify and steal by insiders or external attackers, and that information moving between organizations can vary in classification depending on its context in each organization, even if their classification schemes are identical.**[19]**

Media handling section's purpose is to prevent unauthorized disclosure, modification, removal, or destruction of information stored on media. The management of removable media should include procedures for classification, authorization, secure storage, and the use of cryptographic techniques to protect data. Formal procedures for the secure disposal of media should be established to minimize the risk of confidential information leakage to unauthorized persons. Media containing information should be protected against unauthorized access, misuse, or corruption during transportation. Logs should be kept to identify the content of the media, the protection applied, and the transfer times to maintain an audit trail. When confidential information on media is not encrypted, additional physical protection of the media should be considered. The implementation of these controls should be documented, and procedures and authorization levels should be established.**[19]**

5. **Access control:** It has 4 sections: business requirements of access control, access to networks and network services, use of secret authentication information, system and application access control.

   The **business requirements of access control** section covers the business requirements of access control. The objective is to limit access to information and information processing facilities. An access control policy should be established, documented, and reviewed based on business and information security requirements. Asset owners should determine appropriate access control rules, access rights, and restrictions for specific user roles towards their assets, reflecting the associated information security risks. The policy should take account of security requirements of business applications, information dissemination and authorization policies, consistency between access rights and information classification policies, relevant legislation and contractual obligations, management of access rights in a distributed and networked environment, segregation of access control roles, formal authorization of access requests, periodic review of access rights, removal of access rights, archiving of records of all significant events concerning the use and management of user identities and secret authentication information, and roles with privileged access. Care should be taken when specifying access control rules, and access control rules should be supported by formal procedures and defined responsibilities. Role-based access control is an approach used successfully by many organizations to link access rights with business roles. Users should only be provided with access to the network and network services that they have been specifically authorized to use, and a policy should be formulated concerning the use of networks and network services. The policy should cover networks and network services that are allowed to be accessed, authorization procedures, management controls and procedures, means used to access networks and network services, user authentication requirements, and monitoring of the use of network services. The policy on the use of network services should be consistent with the organization's access control policy. Unauthorized and insecure connections to network services can affect the whole organization, and this control is particularly important for network connections to sensitive or critical business applications or to users in high-risk locations.**[19]**

6. **Cryptography:** This chapter is about cryptographic controls. It discusses the use of cryptographic controls to protect the confidentiality, authenticity, and integrity of information. It suggests that organizations should develop and implement a policy on the use of cryptographic controls for information protection. The policy should consider various factors such as the management approach, risk assessment, key management, and regulatory compliance. It also highlights the importance of specialist advice in selecting appropriate cryptographic controls. The passage further emphasizes that a key management system should be established for generating, storing, archiving, retrieving, distributing, retiring, and destroying cryptographic keys. The system should be based on an agreed set of standards, procedures, and secure methods. Finally, the passage recommends that organizations should define activation and deactivation dates for keys to reduce the likelihood of improper use.**[19]**

7. **Physical and environmental security:** This section consists of these controls: secure areas and equipment.

Secure areas control provides guidelines for the information security management of an organization. The text outlines the physical security measures that should be taken to prevent unauthorized physical access, damage, and interference with the organization's information and information processing facilities. The text emphasizes the need for security perimeters, physical entry controls, securing offices, rooms, and facilities, and protecting against external and environmental threats. The implementation guidance provided in the text includes recommendations such as defining security perimeters based on a risk assessment, restricting access to authorized personnel only, maintaining records of visitor entry and exit, and wearing visible identification. The text concludes that specialist advice should be sought to avoid damage from natural disasters and human error.**[19]**

Equipment control is about information security management systems. The passage deals with the protection of equipment used to process or store sensitive information. The objective of the guidelines is to prevent the loss, damage, theft, or compromise of assets and interruption to the organization’s operations. The guidelines cover the siting and protection of equipment to minimize the risks from environmental threats and hazards, supporting utilities, cabling security, equipment maintenance, and removal of assets. Implementation guidance for each of these controls is provided. The passage emphasizes the importance of regular inspections and testing of equipment to ensure its proper functioning, only authorized maintenance personnel to carry out repairs and service equipment, and the need to prevent unauthorized removal of assets.**[19]**

8. **Operations security:** It has multiple controls: operational procedures and responsibilities, protection from malware, backup, logging and monitoring, control of operational software, technical vulnerability management and information systems audit considerations.

   Operational procedures focus on operational procedures and responsibilities to ensure correct and secure operations of information processing facilities. The control suggests documenting procedures for operational activities and treating them as formal documents, with changes authorized by management. Changes to the organization, business processes, information processing facilities and systems that affect information security should be controlled, and capacity management should be implemented to monitor, tune and project future capacity requirements to ensure required system performance. Additionally, development, testing, and operational environments should be separated to reduce the risks of unauthorized access or changes to the operational environment. Inadequate control of changes to information processing facilities and systems is a common cause of system or security failures.**[19]**

Protection from malware control ensures that information and information processing facilities are protected against malware. This can be achieved through the implementation of detection, prevention, and recovery controls, combined with appropriate user awareness. It provides guidance for implementing controls against malware, including establishing a formal policy to prohibit unauthorized software, implementing controls to prevent or detect the use of malicious websites, reducing vulnerabilities through technical vulnerability management, installing and regularly updating malware detection and repair software, defining procedures and responsibilities for dealing with malware protection, preparing business continuity plans for recovering from malware attacks and implementing procedures to regularly collect information about new malware. The use of multiple software products from different vendors can improve the effectiveness of malware protection, but care should be taken to protect against the introduction of malware during maintenance and emergency procedures. It also acknowledges that the use of malware detection and repair software alone is not usually adequate and commonly needs to be accompanied by operating procedures that prevent the introduction of malware.**[19]**

Backup chapter recommends taking and testing regular backup copies of information, software, and system images to protect against data loss. An organization should establish a backup policy to define its backup requirements, including retention and protection. Adequate backup facilities should be provided, and the backups should be stored remotely with appropriate physical and environmental protection. Regular testing of backup media and restoration procedures should be conducted. Operational procedures should monitor the execution of backups, and backup arrangements for critical systems and services should cover all necessary information, applications, and data. The retention period for essential business information should also be determined.**[19]**

Logging and monitoring objectives are to record events and generate evidence for user activities and other events through logging and monitoring. Event logs should include relevant information such as user IDs, system activities, key events, system access attempts, changes to system configuration, and records of transactions executed by users in applications. Logging facilities and log information should be protected against tampering and unauthorized access, while system administrator and system operator activities should also be logged and regularly reviewed. Clock synchronization is also important to ensure the accuracy of audit logs for investigations or as evidence in legal or disciplinary cases. However, event logs can contain sensitive data and personally identifiable information, so appropriate privacy protection measures should be taken. Additionally, system administrators should not have permission to erase or deactivate logs of their own activities, and the copying of appropriate message types to a second log or the use of suitable system utilities or audit tools should be considered to help identify significant events for information security monitoring purposes.**[19]**

Control of operational software control is about ensuring the integrity of operational systems by implementing procedures to control the installation of software on these systems. The standard provides guidelines for controlling changes in software, including updating operational software, applications, and program libraries by trained administrators upon appropriate management authorization. The standard recommends maintaining previous versions of application software and vendor-supplied software used in operational systems should be maintained at a level supported by the supplier. Any decision to upgrade to a new release should take into account the business requirements for the change and the security of the release. Access to suppliers for support purposes should only be given, when necessary, with management approval, and the supplier's activities should be monitored. Computer software can rely on externally supplied software and modules, which should be monitored and controlled to avoid unauthorized changes that could introduce security weaknesses.**[19]**

Technical vulnerability management chapter is about the prevention of the exploitation of technical vulnerabilities in information systems. To achieve this objective, the standard recommends that organizations obtain timely information about technical vulnerabilities, evaluate their exposure to such vulnerabilities, and take appropriate measures to address associated risks. This includes defining roles and responsibilities for technical vulnerability management, identifying relevant technical vulnerabilities, establishing a timeline to react to notifications, identifying associated risks and taking action, testing and evaluating patches before installation, and keeping an audit log for all procedures. The organization should also restrict software installation by establishing and enforcing strict policies to prevent the introduction of vulnerabilities that could lead to information security incidents or violations of intellectual property rights. **[19]**

Information systems audit considerations section aims to minimize the disruption caused by audit activities on operational systems. The implementation guidance suggests that audit requirements for accessing systems and data should be agreed upon with the appropriate management. The scope of technical audit tests should also be agreed upon and controlled and should have read-only rights. Requirements for special or additional processing should be identified and agreed upon. Audit tests that could affect system availability should be run outside business hours, and all access should be monitored and logged to produce a reference trail.**[19]**

9. **Communications security:** This section consists of these controls: Network security management, Information transfer.

   Network security management control includes establishing responsibilities and procedures for networking equipment management, separating operational responsibility for networks from computer operations, establishing special controls for data confidentiality and integrity over public or wireless networks, implementing appropriate logging and monitoring, authenticating systems on the network, and restricting system connections to the network. Additionally, security mechanisms, service levels, and management requirements of all network services should be identified and included in network services agreements, and groups of information services, users, and information systems should be segregated on networks. In this document, it is also suggested that wireless networks require special treatment due to the poorly defined network perimeter and that extensions beyond organizational boundaries can increase the risk of unauthorized access to sensitive or critical information systems.**[19]**

Information transfer section focuses on maintaining the security of information transfer within an organization and with external entities. To achieve this, formal transfer policies, procedures, and controls must be in place. Procedures should be designed to protect information from interception, copying, modification, misrouting, and destruction. Cryptographic techniques should be used to protect the confidentiality, integrity, and authenticity of information. Information transfer agreements should incorporate management responsibilities for controlling and notifying transmission, dispatch, and receipt. Policies, procedures, and standards should be established and maintained to protect information and physical media in transit. Finally, confidentiality or non-disclosure agreements reflecting the organization's needs for information protection should be identified, regularly reviewed, and documented.**[19]**

10. **System acquisition, development and maintenance:** This section consists of these controls: Security requirements of information systems, Security in development and support processes, and Test data.

    Security requirements of information systems discuss the security need to include information security in all aspects of the system's lifecycle. This includes analyzing and specifying security requirements and controls, identifying and managing security requirements, and integrating security into the design stage to create more cost-effective solutions. The passage also touches on securing application services on public networks, which includes protecting information from fraudulent activity and unauthorized access. The implementation of cryptographic controls is often necessary to ensure the confidentiality, integrity, and availability of information, particularly in applications accessible via public networks. The passage emphasizes the importance of a formal testing and acquisition process when acquiring products, and defines criteria for accepting products. The passage concludes by highlighting the need to protect information involved in application service transactions from fraudulent activity, contract disputes, and unauthorized disclosure and modification.**[19]**

Security in development and support processes focuses on security in development and support processes for information systems. It provides guidelines and implementation guidance to ensure that information security is designed and implemented throughout the development lifecycle of information systems. The section includes controls such as secure development policy, system change control procedures, technical review of applications after operating platform changes, and restrictions on changes to software packages. Secure programming techniques should be used both for new developments and in code reuse scenarios where the standards applied to development may not be known or were not consistent with current best practices. Organizations should ensure that changes to systems within the development lifecycle are controlled by formal change control procedures to ensure the integrity of systems, applications, and products from the early design stages through all subsequent maintenance efforts. [19]

Test data chapter is about securing the data that is taken for testing. It recommends careful selection, protection, and control of test data. The use of operational data containing personally identifiable information or other confidential information for testing should be avoided, but if necessary, sensitive information should be protected by removal or modification. Access control procedures, separate authorization, erasing operational information after testing, and logging of activities should be implemented to protect operational data used for testing. Although substantial volumes of test data are required for system and acceptance testing, efforts must be made to ensure that test data are as close as possible to operational data while being protected. [19]

11. **Supplier relationships:** This section consists of these controls: Information security in supplier relationships and Supplier service delivery management.

    Information security in supplier relationships objective is to ensure the protection of an organization's assets that are accessible by suppliers. The guidelines outline information security policies for supplier relationships and address security within supplier agreements. They recommend identifying and mandating information security controls for supplier access to an organization's information in a policy. The controls should address processes and procedures to be implemented by the organization, as well as those processes and procedures that the organization should require the supplier to implement. The guidelines also recommend establishing and documenting supplier agreements to ensure that there is no misunderstanding between the organization and the supplier regarding information security requirements. The agreements should include information on the classification of information, legal and regulatory requirements, access control, incident management, and defect resolution.[19]

    Supplier service delivery management objective is how to maintain an agreed level of information security and service delivery in line with supplier agreements. To achieve this objective, organizations should regularly monitor, review and audit supplier service delivery to ensure adherence to information security terms and conditions of agreements, proper management of information security incidents and problems, and sufficient service capability to maintain agreed service continuity levels following major service failures or disasters. Sufficient technical skills and resources should be made available to monitor compliance with information security requirements, and appropriate action should be taken when deficiencies in service delivery are observed. Additionally, changes to supplier services, including maintaining and improving existing information security policies, procedures and controls, should be managed to take into account the criticality of business information, systems, and processes involved, and re-assessment of risks.[19]
12. **Information security incident management:** This section consists of the Management of information security incidents and improvements control.

This section outlines the guidelines for the management of information security incidents, including responsibilities and procedures for incident response planning, preparation, monitoring, detecting, analyzing, reporting, logging, managing forensic evidence, assessing events, and decision-making. Reporting and assessing security weaknesses, responding to incidents by collecting evidence, analyzing, and controlling the situation, coordinating with relevant personnel and external parties, and communicating internally and externally is also crucial. The responsibility of personnel in reporting and preventing incidents, and the importance of quick, effective, and orderly response is emphasized. The section also acknowledges the need for coordination and information sharing among external organizations. **[19]**

13. **Information security aspects of business continuity management:** This section consists of these controls: information security continuity and redundancies.

Information security continuity is a chapter about how the organization should determine the requirements for information security and the continuity of information security management in adverse situations, and establish processes, procedures, and controls to ensure the required level of continuity for information security during an adverse situation. The organization should also verify, review, and evaluate information security continuity controls at regular intervals. It is recommended to capture information security aspects within normal business continuity management or disaster recovery management processes. The organization should involve information security specialists when establishing, implementing, and maintaining business continuity or disaster recovery processes and procedures. The verification of information security continuity controls should be performed outside the testing of changes, and it is preferable to integrate it with the organization's business continuity or disaster recovery tests.**[19]**

Redundancies chapter provides guidance for information security management and includes control objectives and implementation guidance for information security continuity and redundancies. The objective of this section is to ensure the availability of information processing facilities. The control requires that information processing facilities are implemented with redundancy sufficient to meet availability requirements. Organizations should identify business requirements for the availability of information systems and consider redundant components or architectures where the existing systems architecture cannot guarantee availability. Redundant information systems should be tested to ensure that failover from one component to another works as intended. However, redundancies can introduce risks to the integrity or confidentiality of information and information systems, which must be considered during their design.**[19]**

For this company, the controls were chosen to cover necessary risks they potentially face and provide guidelines on how to manage the small infrastructure they possess. To address the risks in this company and provide policies for better operation and security, the following controls were taken into account: Information security in project management, Mobile devices, User access management and teleworking, Information classification, Business requirements of access control, Operational procedures and responsibilities, Responsibility for assets, Business requirements of access control, Secure areas, Event logging.

3 Methodology

This chapter explains how the research was conducted and what methods were used for it. It includes research methods, data analysis and collection methods, and the development of an information security management system for Samleks OÜ.

3.1 Research methods

For this research it was important to be familiar with ISO 27001 standard and the medical industry, specifically the aesthetic medicine branch. The method chosen for this study was qualitative research. Such a method was chosen due to data being collected through a survey.

Theoretical knowledge was obtained through various books, articles, documentation, and official websites.

3.2 Data analysis and collection methods

To collect data about current information security in this company, the author has conducted a survey consisting of 10 questions in English. The survey was completed by the financial manager and the sales manager. Currently, Samleks OÜ consists of two people, and there is no IT specialist in the company. The survey was done in the office on the spot and answers were written down in Notepad. This survey aimed to understand how information security works in Samleks OÜ.

Survey questions with answers:

1. **Who manages new users' information, who want to register an account and how new users accounts are managed and considered in the company's overall management?**

They can register themselves if they are regular users. The ones who want to access professional products need to send an email with the company information. Products can be bought without having an account, too. There is no set process for how new users are managed.

2. What importance does the Webpage with the associated information system serve to the company?

For people to be aware of this company, for advertisement purposes, and also for schooling information. The necessary contact information.

3. What is the webpage availability requirement?

The aim is to always have it available and in case of downtime, there is an email sent to them.

4. What information is stored about users and how long is it retained? In cases of inactive accounts, is there some deletion time or process with deletion time, or is there some solution for when and how the actual personal data will obfuscate?

There are no rules about deletion, all accounts are stored, no matter how active they are. The saved information is used to send out advertisements and sales and deals (the email). Depending on the type of user, medical license is saved.

5. Is there any sensitive information about customers stored? If yes then, where precisely is the information about registered customers stored?

No there is no, they have an agreement with the banking companies that the payment is redirected there through a banking link.

6. Which measures and according to which standards have been done to secure the payments on a website, which measures?

They have a contract with a bank that does it for them. They have not implemented any standards.

7. How does the company ensure the confidentiality, integrity, and availability of customer data and transactions on the website?

The transactions are made secure with a contract with banks, but for the other aspects, they have not taken any measures.

8. How and by whom is data backup and recovery managed, and how frequently are backups performed?

The webpage is done in WordPress, and the backup is done once a day by Zone EE. There were no prior backups done until an incident happened where the page lost all data and was out of service.

9. What security measures are set in place to prevent unauthorized access to the website and its databases?

There are no specific measures in place, no IT professional has been hired, and the only person who has access to the page is the finance manager.

10. What security risks are you aware of that potentially targets your company?

They are not aware of any security risks.

4 Results and Analysis

This chapter provides an overview of the practical part of the research and the end result. In this section, there is an ISMS for this company and an analysis of the work that has been done.

4.1 Development of information security management system for Samleks OÜ

The ISO/IEC 27001 standard is made for organizations to use as a reference for selecting controls within the process of implementing an Information Security Management System (ISMS) based on ISO/IEC 27001 or as a guidance document for organizations implementing commonly accepted information security controls.[19]

For developing an ISMS for a specific company, it is important to understand what the business is about, what its values are, and who has responsibilities for certain functions in the system. This chapter also explains each of the necessary documents in theory, and why they are necessary to have for ISMS that is developed for a smaller company like Samleks OÜ.

The important documents and records of the ISMS that will be covered during this development are the following:

- Information Security Scope
- Information security policy and objectives
- Risk Assessment and risk treatment methodology
- Definition of Security Roles and Responsibilities
- Inventory of Assets
- Acceptable Use of Assets
- Access Control Policy
- Incident Management Procedure
- Business Continuity Procedures
- Internal audit program

As this research focuses only on the theoretical parts of the development of an information security management system, any documents that require practical implementation, such as policy implementation, will not be included. Some of the parts are also excluded due to the nature of this organization (small infrastructure and small amount company members). [20]

4.1.1 Information Security Scope

The scope of this ISMS includes the management of information security for the online store that sells aesthetic medicine products. This includes the handling of the personal information of registered users, such as their full name and email, as well as any sensitive information related to payment transactions. They also require medical licence from customers who are ordering professional grade products and they are stored for further purchases from these clients. The ISMS aims to ensure the confidentiality, integrity, and availability of this information, and to comply with any relevant legal or regulatory requirements related to information security. To further understand the full scope, the company's goals and target demographic will be explained. [20]

The aesthetic medicine company Samleks OÜ was formed in 2016 and is located in Estonia. The product brands that are sold are from Spain, Italy, and Korea. They are also the distributors of GENYAL (Xcelens International Sagl, Switzerland) in Estonia, Finland, and Sweden.

The company also organizes masterclasses for professional cosmeticians and aesthetic medicine practitioners. Overall, the main targets are aesthetic medicine clinics and cosmetologists, although some of the products can be bought by regular users too. The orders are mainly from Europe, and they plan on selling worldwide.

Their mission is to provide high-quality products for enhancing the beauty and well-being of their clients. They aspire to compete more effectively with their rivals in the highly competitive market by continuously improving their products and services.[21]

The infrastructure of the company is quite small and does not consist of many devices since they do not handle large amounts of data. There is an office that consists of two small rooms, and each has one laptop per person. The devices do not leave the office, they are for spot use. They also have a Wi-Fi router, there is no public Wi-Fi in the building, and each company has to provide its own internet access. For working with clients, they also use personal phones, usually for calls. The IT part of the company is managed solely by the financial manager. They also have a printer that is used occasionally.

4.1.2 Information security policy and Objectives

At Samleks OÜ, they are committed to ensuring the confidentiality, integrity, and availability of information and information systems used in their operations. As such, they will establish an Information Security Management System (ISMS) that is based on the ISO 27001 standard.

ISMS policy for Samleks OÜ is built upon the following principles:

- Information security is an integral part of business processes and operations. The company will ensure that information security is integrated into all aspects of the organization, including its products, services, and internal processes.

- Company will identify and assess the risks associated with existing information systems and take appropriate measures to mitigate those risks. This includes regularly reviewing risk assessment and management processes to ensure that they remain effective and up-to-date.

- Company will comply with all relevant legal and regulatory requirements related to information security, including obtaining necessary certifications and registrations such as the CE certificate for products and registration of products in the health board.

- Company will ensure that all employees, contractors, and third-party service providers are aware of information security policies and understand their roles and responsibilities in maintaining the security of company information systems.

- Company will regularly monitor and review the effectiveness of ISMS and information security controls to ensure they meet Samleks OÜ business needs and objectives.

- Company will ensure that all incidents and breaches related to information security are promptly reported and investigated, and appropriate measures are taken to prevent similar incidents in the future.

- Company will continuously improve their ISMS by regularly reviewing and updating policies, procedures, and controls to reflect changes in business processes, technology, and the threat landscape.

By adhering to these principles, the company will ensure that its information systems remain secure and resilient against threats and that they continue to provide customers with high-quality products and services that meet their needs and expectations. [20][22]

4.1.3 Risk Assessment and risk treatment methodology and Report

The purpose of this chapter is to assess the different types of risks that Samleks OÜ faces. It provides an overview of the risks that can potentially harm the company, and it outlines the steps that should be taken to manage those risks. The scope of this chapter is to focus on information security, operational, and financial risks, which are the most relevant to the organization. Further, the risks are explained. The assets of the company will also be discussed. [23]

The organization faces various types of risks that can potentially harm its operations and reputation. Information security risk is one of the most significant risks that the organization faces, which can lead to data breaches, theft of confidential information, and other cyber-attacks. This organization also faces operational risks, such as the risk of human errors, natural disasters, and system failures. Furthermore, the organization faces financial risks, such as the risk of bankruptcy, debt, and other financial losses. [23]

Information security risks pose a significant threat to the organization's operations and reputation. These risks can come from various sources, including internal and external ones. They can lead to data breaches, the theft of confidential information, and other forms of cyber-attacks. To mitigate these risks, the organization should implement robust information security measures, such as managing who can access what, data encryption, and planned security audits that are done regularly.[23]

Operational risks are inherent in any organization's operations and can arise from various sources. For example, human errors, system failures, and natural disasters can all disrupt the organization's operations and lead to financial losses. To mitigate these risks, the organization should have contingency plans and backup systems in place to ensure that operations can continue in the event of a disruption.[23]

The financial risks can also have a significant impact on the organization's operations and reputation. These risks can arise from various sources, such as bankruptcy, debt, and other financial losses. To mitigate these risks, the company should have clear financial management practices in place. For example, regular financial audits, debt management, and risk analysis.[23]

In addition to the risks identified earlier, there is another emerging risk that the organization should be aware of: the Internet of Things (IoT). IoT describes physical objects that are connected within a network, they have sensors, software, and other technologies embedded. While IoT may offer many benefits, for example, increased efficiency and productivity, it also introduces security risks. If the organization is planning to grow and expands its operations, it may consider implementing IoT devices to streamline processes and improve operations. However, it is important to be cautious with it and to prioritize security measures to mitigate the potential risks.[23]

In conclusion, the organization faces various types of risks, including information security risks, operational risks, and financial risks. To minimize these risks, the organization should implement robust risk management practices, such as access controls, emergency plans, and sound financial management practices. [23]

The following part of this risk assessment is about the method that was chosen to further evaluate the risks.

The risk assessment methodology is an important component of the organization's ISMS. It involves identifying, evaluating, and prioritizing potential risks to the organization's assets and determining the probability and impact of those risks.

A commonly used method would be the "asset-threat-vulnerability" methodology is a widely used risk assessment method that can help organizations identify, evaluate, and prioritize potential risks to their assets. According to NIST Special Publication 800-30 Revision 1, this methodology involves three main components: assets, threats, and vulnerabilities. Assets are all the valuable parts of the company, like devices, systems and so on. Threats are the potential sources which harm a company's assets can originate from. Lastly, vulnerabilities are exploitable faults in the system that can be used in a way to harm the assets of the company that are necessary for its processes. Once the assets, threats, and vulnerabilities have been identified and evaluated, the next step is to develop appropriate risk mitigation strategies. The asset-threat-vulnerability methodology can be particularly useful for organizations with complex infrastructures and a wide range of assets and processes. However, for small organizations with limited resources and infrastructure, a simpler and more practical risk assessment methodology, such as the "likelihood-impact-mitigation" method, may be more appropriate.[24]

The "likelihood-impact-mitigation" methodology is a widely used risk assessment approach that is particularly well-suited for small companies with limited resources and infrastructure. This methodology involves assessing the likelihood and impact of identified risks and determining appropriate mitigation strategies to reduce the probability and impact of those risks. According to NIST SP 800-30 Revision 1, the "likelihood" of a risk is the probability that it will occur, while the "impact" of a risk is the magnitude of harm that could result if the risk were to occur. In this methodology, both the likelihood and impact of identified risks are assigned numerical values and are used to create a risk matrix. This matrix can help determine the appropriate mitigation strategy based on the risk's likelihood and impact scores.[24]

Ultimately, the chosen risk assessment methodology will be tailored to the organization's unique needs, resources, and risk tolerance. It has to be regularly reviewed and updated to reflect changes in the organization's infrastructure, operations, and risk environment. With this particular organization, the changes that happen in its environment are minimal, and most likely the already set methodology does not have to be reviewed often.

For this small company with limited resources and infrastructure, the author chose the "likelihood-impact-mitigation" approach, which is better suited for the risk assessment methodology in this company. This methodology is less complex and more practical than the "asset-threat-vulnerability" method. This approach is a more efficient use of resources and allows for a focused analysis of the company's specific risks. Taking into account that the organization has limited resources and staff. The risk matrix is illustrated in the Table below, where 1 means very low probability and 5 is a very high probability. The highest risk level that can occur is 25. [25]

Table 2: Risk matrix table [26]

Asset	Threat	Vulnerability	Impact	Likelihood	Risk Level	Mitigation Strategy
Laptops	Theft	Unauthorized access to	5	3	15	Security system for

		sensitive information				entering office
Laptops	Malware, that could be downloaded	Outdated software and operating systems	4	3	12	updating systems, being educated on threat like this
Laptops	Unauthorized access	Weak password	5	2	10	long passwords without predictable patterns, 2FA
Laptops	Insecure Wi-Fi networks	Lack of encryption or strong authentication	4	3	12	encryption of the traffic
Smartphones	Theft or loss	No physical security measures	5	2	10	not leaving the device in unsecured places
Smartphones	Malware	Downloading malicious software or files	4	3	12	updating systems, being educated on threat like this
Smartphones	Unauthorized access	Weak password	4	2	8	long passwords without predictable patterns, 2FA
Smartphones	Insecure Wi-Fi networks	Lack of encryption or strong authentication	4	3	12	encryption of the traffic
Printer	Cyber attack	Lack of proper security settings or updates	5	2	10	updating the system, encryption of the traffic
Cisco IP Phone	Eavesdropping or call data exposure	Vulnerabilities in VoIP protocols	3	3	9	encrypted VoIP protocols
Official webpage	Outdated plugins.	Different cyber-attacks.	4	3	12	regular plugin updates and using security

Products	Extreme temperature changes	Malfunctions in heating system	5	5	25	patches

The infrastructure of the company is quite simple and small, it does not hold many assets that could be harmed or exploited. The devices are the following: two laptops, two Android phones, a Cisco IP phone, and a printer. The laptops are used mostly for everyday purposes, like sending emails. The financial manager also uses it for finance and managing the organization's webpage. Applications that are in use for communication with clients are generic social media platforms.

There are still many potential risks, considering the organization's small infrastructure, and they would be the following:

- **Laptops:** the risk of the device being stolen from the office may result in unauthorized access to sensitive information; any malicious software or files could be downloaded onto them and then spread further, insecure Wi-Fi networks could be accessed, putting company data at risk of interception; outdated software and operating systems could be vulnerable to various attacks.
- **Smartphones:** devices could also be lost or stolen, since their size is smaller than laptops it has a high likelihood, this puts sensitive data at risk even if they are protected by a password. Similarly, to laptops, Wi-Fi networks could be accessed, putting company data at risk of interception. The possibility of downloading something malicious is also there.
- **Printer:** It is connected to the Wi-Fi network it can be vulnerable similarly to previous devices. In case of printer falls under attack, it serves as a gateway for an attacker to get inside a network.
- **Cisco IP Phone:** the vulnerable expect of this device is VoIP which could potentially expose the call data, or someone can eavesdrop.
- **Official web page:** it may fall under cyber-attack and data about registered clients there can get compromised, web page has some issues as the plugins are soon outdated.

- **Heating system:** in case of malfunction the product can spoil.

4.1.4 Security Roles and Responsibilities

In order to define the security roles and responsibilities for Samleks OÜ, it is important to first understand the company's infrastructure and its operations. As a small company with limited resources, it is important to keep security policies and procedures as clear and concise as possible. [19]

The security roles and responsibilities should be defined in a way that is specific and measurable, with clear expectations for all individuals involved in the company's operations. These roles and responsibilities should be outlined in the company's policies and procedures, with specific details on who is responsible for what tasks related to security. [19]

Given that the IT part of the company is managed solely by the financial manager, it is important to clearly outline their security responsibilities, including managing access control, performing regular backups, and ensuring that all devices are secure and up to date with software patches and updates. [19]

Third-party security roles and responsibilities should also be defined in any contracts the company enters into, particularly in cases where sensitive information is being shared with external parties.[19]

It is also important to consider the potential risks and threats to the company's operations and assets, ensuring that security policies and procedures are in place to mitigate those risks. In order for policies to remain relevant and effective over time, they should be updated and reviewed.[19]

The following responsibilities fall on the financial manager:

- **Information security management:** The financial manager would be responsible for managing and overseeing the overall information security of the company's IT infrastructure, including hardware, software, networks, and data.

- **Access control:** The financial manager would be responsible for managing access to the company's web page.

- **Data backup and recovery:** The financial manager would be responsible for ensuring that the company's data is backed up regularly and securely and that there are processes in place for recovering data in case of system failures or data loss.

- **Incident response:** The financial manager would be responsible for managing and responding to any security incidents that occur, including identifying and containing the incident, investigating the cause, and implementing corrective actions to minimize the possibility of it happening again.

- **Security awareness and training:** The financial manager would be responsible for ensuring that all employees of the company are aware of their security responsibilities and that they receive regular training on information security best practices and procedures.

- **Vendor management:** The financial manager would be responsible for managing the security of any third-party vendors or contractors that the company works with, including reviewing and approving security policies and procedures, and ensuring that they comply with the company's security requirements. [19]

4.1.5 Inventory of Assets

An inventory of assets is a crucial aspect of any ISMS. It involves identifying and documenting all the assets within an organization that need to be protected. These assets may include hardware, software, data, and even personnel. [19][20]

Generally, it is important to conduct an inventory of assets in order to develop an ISMS. It aids the company to understand what needs protecting and how it is possible to protect it. By doing that, it improves their overall security. [19]

In the case of Samleks OÜ, their infrastructure is relatively small and simple. Therefore, the inventory of assets should be relatively simple as well. The following is a list of assets that should be considered for Samleks OÜ:

- **Hardware:** This includes the laptops, cisco ip phone, printer, and the Wi-Fi router that is in the company’s use in their office. The company's devices also include smartphones, which are used for communication with clients.

- **Software:** The company uses various software applications for neccecary business processes, separate for accounting and communication with clients. Phones are mostly used for communication through the application that has been covered in the Risk assessment chapter.

- **Data:** This includes all the data that the company stores, processes, or transmits. More specifically client data, financial data, and any other confidential data that is relevant to their business. In this case, the user's email and full name are stored. Additionally, customers who want to purchase professional products must provide their medical license in order to verify that they are allowed to use it and it is also stored. When clinics want to purchase any products, they also have to provide details about their company which would be stored for future purchases from the clinic.

- **Personnel:** Even if the company is small, it is important to document the roles and responsibilities of all the employees who have access to the company's assets. Including the financial manager who manages the IT part of the company. [27][28]

4.1.6 Acceptable Use of Assets

This policy outlines the acceptable use of company-owned IT assets by employees and third-party contractors. This policy applies to all IT assets that are owned by this company, which include laptops, smartphones, printers, and other electronic devices. [20] [19]

The purpose of this policy is to make sure that the proper use of company-owned IT assets protects the company's information, systems, and the privacy of employees, clients, and partners. The policy ensures compliance with laws, regulations, and contractual obligations. It also ensures the productivity and efficiency of employees. [19]

These following rules apply to the acceptable use of company-owned IT assets:

Ownership and Responsibility:

- All company-owned IT assets are the property of the organization and must be used only for authorized business purposes.
- Employees and contractors of the company are responsible for the proper use and protection of company-owned IT assets.

Prohibited Activities:

- The following activities are prohibited on company-owned IT assets.
- Using company devices for personal purposes.
- For example, browsing social media, online shopping, and personal email.
- Installing or using unauthorized software or hardware that has not been approved by the company.
- Giving unauthorized individuals access to sensitive or secret information.
- Actions that go against rules, policies, or regulations set by the company.
- Using IT assets for unethical reasons.

Security Measures:

- Employees and contractors of the company must take the necessary security measures to protect company-owned IT assets, which are listed further.
- Using complicated passwords that would not be easily guessed, changing them often, and in case of need, having a password vault.
- Locking the devices when not in sight or leaving the room.
- If there is a suspicion that an incident may have happened, it has to be reported immediately to the financial manager.
- Having awareness of when devices have regular updates and scheduling them on devices that need it.
- Using anti-virus software and performing updates on it.

Monitoring and Enforcement:

- The company must monitor and review its assets and ensure that everything is following its policies. In the case of a violation, the company has the right to take disciplinary action. They include termination of the contract or legal action. [28]

To conclude, all company members and third-party contractors must comply with these policies. In case of violation, it must be reported to the financial manager.

4.1.7 Access control policy

The Access Control Policy outlines the procedures and guidelines for managing access to the company's information systems, assets, and data. The purpose of this access policy is to secure access to Samleks OÜ owned assets. This ensures that only authorized individuals can access the information and devices. This policy's purpose is also to safeguard the company's information against unauthorized access, theft, or misuse. It applies to all parties inside the company and other contractors that they are working with. [19][20]

The scope of this policy covers physical and logical access control. Logical access includes the authority of users who want to access specific information or devices. Physical access control includes the ways security has been implemented to secure the company's working grounds and prevent any outside access that has not been approved. [19][28]

In this policy, access control is based on multiple principles that have guidelines for how access should be granted, monitored, and managed. Users with the fewest privileges have access to only the necessary data and information, in order to perform their daily job tasks. In this company, the highest privileges belong to the financial manager, and the least privileges belong to the sales manager.[19][28]

Access control procedures are the policies and processes that are put in place to manage user access to information systems and data. These include when someone is requesting access to information that they have not been granted privileges to. It specifies what the procedure is, how to request it, and in what cases access is denied or granted. Access control procedures explain how they are regularly reviewed and revoked when deemed necessary. User authentication and password policies are also essential components of access control procedures.[19][28]

Logical access control includes the implementation of measures that restrict access to specific systems, applications, and data for security. A common approach for such is role-based access control. In this case, access is granted according to the user's job duties and responsibilities. Managing the accounts is also an important aspect, as it defines how they are created and deleted. The access to a company's web page must be carefully controlled, as only one person is allowed to access it, which is financial manager.[19][28]

Physical access control is put in place to secure the physical location such as office, so there would not be any unauthorized access. To apply such measure there must be some sort of access control system like for example keycard systems. Additionally, access to the financial manager's laptop must also be restricted, and the laptop should be secured when not in use. The company already has a key-based system in use.[19][28]

Access control monitoring involves the regular monitoring and auditing of access control measures to ensure that they are effective and secure. These logs must be maintained, in order to have an ovewriew of who acces what and what exactly did they do. Any security incidents should be recorded in same manner and reporting rules should be in place.[19][28]

The effectiveness of access policy control takes effect only when it is actually applied. Clear guidelines on how to act and what processes to follow must be in place so that in the case of a suspected violation, people know how to act accordingly. Consequences must also be defined in the event of a policy violation by any party. [19][28]

Training the company members on this policy is essential to ensuring that they understand the rules and their importance. It also helps to maintain secure practices. To help reinforce the policy, it is crucial to perform awareness campaigns.[19][28]

In summary, these policies must be reviewed and updated on a regular basis to ensure that they still are effective. The frequency of this process depends on the company's needs and is especially important when there is a new member or some sort of relocation or new location. With this company, there is no need to do them frequently as they do not plan to expand or relocate.

4.1.8 Incident Management Procedure

Incidents that put a company's information and data at risk can happen in any organization. It is important to have well-defined incident management procedures in order to ensure that they are handled correctly. In this chapter, the incident management procedures that the organization would follow are covered. This means that the following aspects of the procedure will be covered: reporting, classification, and handling of security incidents. [19][20][28]

The incident reporting part will outline the process for reporting security incidents, including who should be contacted and what information should be provided.

In this particular scenario where there is no dedicated IT department, the incidents should be reported directly to the financial manager, who is responsible for managing the company's IT-related processes. The financial manager can provide a designated email address or phone number for incident reporting, or a dedicated incident reporting form can be created and made available to all employees. This type of way would be more suitable when the company would expand, and at the moment just the financial managers phone number would be sufficient.[28][29]

For all incidents to be reported on time, employees must understand the process behind it and be trained accordingly. The member should be encouraged to report anything suspicious. This whole process should also be reviewed and updated in order for it to remain effective. According to changes in company the time period should be set for reviewing, most likely if no change occurs it does not have to be reviewed often.[28][29]

In the incident classification section, incidents will be classified according to their severity and impact on the organization. This will enable us to prioritize incident response and allocate appropriate resources. There are three severities: low, medium, and high impact. The highest impact would be considered when data of any devices gets compromised, for example, smartphones or laptops. Another high-impact priority incident is considered if devices would be physically harmed or stolen and getting infected with anything malicious. Under medium impact would be considered the following: downtime of the webpage as it helps to attract new clients, electricity outage, or any other related problems. The lowest impact would be anything regarding the printer, as it holds nothing valuable in it and the company can function without it if needed.[28][29]

The incident handling section will outline the procedures for handling incidents within the organization. Since there is no dedicated incident response team, the financial manager will be responsible for managing the incident. Next, the roles and responsibilities of the financial manager in responding to incidents, and detail the steps to be taken to contain and eradicate the incident. [28][29]

As the sole person responsible for incident response in the absence of an incident response team, the financial manager would need to respond to incidents promptly and effectively. The manager would begin by identifying the nature and severity of the incident and prioritizing the response accordingly. They would then take appropriate steps to contain and isolate the incident to prevent further damage, and document all relevant information related to the incident.[28][29]

Once the incident has been contained, the financial manager would proceed with eradicating the incident and restoring any affected systems or data. Throughout the incident response process, the manager would communicate regularly with any affected parties and provide regular updates on the status of the incident.[28][29]

After the incident has been fully resolved, the financial manager would conduct a post-incident review to identify any lessons learned and areas for improvement in the incident response process.[28][29]

The incident Review section will outline the procedures for reviewing incidents, including the collection and analysis of data related to the incident. It will also define how the lessons learned from the incident will be incorporated into the organization's information security management system. The financial manager would have to gather information on how, when, and what could be the cause of the incident. Then it would be analyzed taking into account the set of rules and policies and then make changes accordingly if needed. Human error also has to be taken into account.[28][29]

This part will detail the steps that will be taken to prevent future incidents, including the development of new policies and procedures and the implementation of additional security controls. [28][29]

Firstly the incident would be documented: when, what, and how happened. Then already set rules and policies will be looked over to see if anything has to be updated, modified, or explained more thoroughly.[28][29]

The Incident Management Procedure section outlines the steps for reporting, classifying, and handling security incidents in the organization. The section on incident reporting details how incidents are to be reported to the designated financial manager, including the necessary information to be provided. Incidents will be classified according to their severity and impact on the organization, allowing for prioritization of incident response and allocation of appropriate resources. [28][29]

The section on incident handling describes the procedures for containing and eradicating incidents, as well as the roles and responsibilities of the financial manager in incident response. It also includes guidelines for communication with stakeholders, including when and how incident reports should be shared with company members and customers.[28][29]

The Incident Management Procedure requires the financial manager to follow specific procedures when handling security incidents. The first step is to report the incident to the appropriate stakeholders, including customers. Once the incident is reported, the financial manager must classify the incident based on its severity and impact on the organization. This will help determine the appropriate response and allocation of resources.[28][29]

After classification, the financial manager should initiate the incident response process, which involves containing and eradicating the incident. The financial manager must also document the incident and its response for future reference and analysis.[28][29]

Once the incident has been resolved, the financial manager should conduct a post-incident review to identify any lessons learned and make any necessary adjustments to the incident management process. The financial manager should also communicate with stakeholders regarding the incident, providing information on the incident, the response, and any corrective actions taken to prevent future incidents.[28][29]

The awareness training is made by the financial manager and they are the only person who is responsible for it. The financial manager would determine what areas of information security knowledge are lacking in the company and then choose appropriate programs for further education. [28]

4.1.9 Business Continuity Procedures

The business continuity plan is a set of documented procedures that assist organizations in responding, recovering, resuming, and restoring operations to a predetermined level after a disruption. However, the focus of BCP is primarily on creating plans and procedures, without including the necessary analysis and maintenance that form the foundation for effective contingency planning. These crucial elements of business continuity management are essential for ensuring the success of contingency planning. [30][20]

Business continuity procedures typically consist of a set of defined processes, protocols, and documentation that provide guidance on how to respond and recover from disruptions. These procedures can help minimize the impact on the organization's operations and reputation. There are following parts are included in this business continuity procedure: scope, reference documents, roles and responsibilities, plan activation and deactivation, communication, incident response, recovery plans for activities, disaster recovery plan, required resources and restoring and resuming activities from temporary measures.[30][19]

The scope of this BCP covers critical processes of this company, including financial and sales management. The purpose of this is to ensure the business can continue its processes even after disruptive incidents. Primary users of this plan would be sales and financial managers. [30][19]

The reference documents that are necessary for this plan are the following: Business Continuity Policy, Business Impact Analysis, Business Continuity Strategy and etc. This plan can only work if the company has the previously named documents. [30][19]

Roles and responsibilities in this company, regarding website-related issues are solely on the financial manager since there is no IT professional in the company. In case of urgency, the financial manager is responsible for purchasing the necessary equipment. They both are authorized to manage disruptive incidents.[30][19]

Plan activation will be initiated by the sales or financial manager upon the occurrence of a disruptive incident. The incident will be reported through the Incident Management Procedure, and the appropriate severity level will be assigned based on the impact analysis. Once it's classified, the financial manager will choose appropriate steps to mitigate it and monitor the progress.[30][19]

Plan deactivation comes when business operations are back to normal, then the financial manager will initiate the deactivation of the business continuity plan. The deactivation process will include a review of the incident response and recovery process, as well as a determination of whether any updates or changes to the plan are necessary based on lessons learned. The financial manager will ensure that all necessary documentation related to the incident is updated and stored securely and that all team members are informed of any changes to the plan.[30][19]

The way of communication in this plan is directly through the phone, between the financial manager and sales manager. For other people who got affected during the incident, phone calls and emails are acceptable.[30][19]

Required resources are an essential part of ensuring that the company can resume and respond to any disruptive incident. Both financial and sales managers are needed to solve the situation, but depending on the incident's nature, the financial manager would have the main responsibility. Third-party services would be needed in case of issues with the website that the financial manager is unable to solve on their own. The provided would be the same as where the website is hosted on.[30][19]

The last part of the business continuity plan would be restoring and resuming activities from temporary measures. Once temporary measures have been put in place to respond to a disruption, it is necessary to establish a process for transitioning back to normal operations. Depending on the incident, most of the responsibilities are on the financial manager regarding the IT part. Incident management is more thoroughly explained in the chapter accordingly.[30][19]

4.1.10 Internal audit program

An internal audit program is an important part of every organisation's information security management system, no matter the size. It is indeed simpler to do an internal audit for a smaller company as it not only takes less time but also a smaller cost. It helps to ensure the effectiveness of ISMS in general. In this company, there is no IT department, so the whole responsibility is on the financial manager. Their role is to implement and maintain an internal audit program. This chapter covers the key components of an effective audit and its appliance in this organisation.[20][31]

The scope of the audit program includes all information assets, processes and controls that are important to the organisation's information security.[31] [29]

The objectives of the program should be aligned with the organization's overall goals and risk management strategy. The finance manager should work with relevant stakeholders to establish and communicate the scope and objectives of the audit program.[31]

The audit methodology defines the approach and techniques used to conduct the internal audits. The audit methodology should include procedures for planning, conducting, reporting, and following up on audits. It should also specify the criteria for evaluating the effectiveness of controls and identifying areas for improvement.[32]

The finance manager should plan and execute internal audits under the audit methodology. This includes identifying audit objectives, selecting audit techniques, conducting fieldwork, and documenting findings. The audit plan should be reviewed and approved by relevant stakeholders before the audit is executed. The finance manager should ensure that the audits are conducted objectively, independently, and without bias.[32]

The finance manager should prepare and distribute audit reports that communicate the audit findings, conclusions, and recommendations to relevant stakeholders. The reports should be clear and understandable. The finance manager should follow up on the audit findings to ensure that corrective actions are taken in a timely and effective manner. The finance manager should also track and report on the status of corrective actions to relevant stakeholders.[32]

The finance manager should continuously monitor and improve the internal audit program to ensure that it remains effective and efficient. This includes conducting periodic reviews of the audit methodology, audit plan, and audit reports. The finance manager should also solicit feedback from relevant stakeholders to identify areas for improvement. The finance manager should ensure that the internal audit program is aligned with the organization's changing needs and risk profile. Since the company is not planning on any changes the regularity of review is not as important. [19]

The finance manager may use a variety of audit tools and techniques to support the internal audit program. The finance manager should select and use audit tools and techniques that are appropriate to the organization's needs and resources. In this scenario, it is more appropriate to use spreadsheets as it is more convenient for the company.

The role of the financial manager is to clearly define the responsibilities of others in the company who are involved in the internal audit program. This includes the sales manager and relevant stakeholders. The importance of the audit program is to make sure that all personnel is equipped to perform their work duties safely in the company.

An effective internal audit program provides the integrity and security of an organization's information assets. Since the company does not have an IT department, the biggest responsibility falls onto the financial manager to maintain the internal audit program.

4.2 Implications for Medical Aesthetics Industry

In companies that provide services and have to store the data of patients for regulatory reasons have to have very strict policies for accessing, using and maintaining the data regarding it. Not all such companies provide services but can also sell products and devices for them instead, so there no patient information. In order for them to make sure the organisation or person who would like to purchase it has legal right to own it, there has to be appropriate licenses provided. On those licences there is personal information such as full name, identification number and more such data. It is crucial to both protect medical licences and personal health data. Problem with smaller companies is their attitude for information security, they might think that because of their size they would not be targeted by various cyber-attacks. Moreover, they might not have dedicated IT specialist in the company to deal with it.

4.3 Recommendations for Samleks OÜ

The main problem in this organisation was lack of knowledge regarding information security and other IT related risks and problems. They should either hire someone temporarily to deal with these aspects or financial manager should get education from some schoolings or courses in to be able to grasp the importance of not only information security but protecting all data generated and retained in the company. It all does come down to actual resources they can allocate for such measures as the research servers as an advisory and even implementing some parts of the ISMS that is affordable for them, secures the processes they chose to apply it to.

5 Summary

The main objective of this thesis was to develop an Information Security Management System (ISMS) for a small aesthetic medicine company based on the ISO 27001 controls. To achieve this objective, various documents and controls were used to develop the ISMS, which is discussed in detail in this research paper.

Firstly, the company's information security practices were evaluated through a small survey to gain an understanding of their current policies and practices. Then, the ISO 27001 controls and categories were analysed to determine which ones would be suitable for the company and to address their existing vulnerabilities. This process included defining the scope of the ISMS, identifying the company's assets, assessing the risks associated with those assets, and identifying measures that can be taken to mitigate those risks. Additionally, the responsibilities of company members, incident management, and the auditing program were also defined as part of the ISMS.

To visually represent the company's most valuable assets that cannot tolerate any downtime, a risk matrix was created. Proposed solutions were provided to secure those assets and the conclusion provides an overview of all the company's assets in general.

It is important to note that smaller companies may not always have the funds to allocate for IT services and security. Therefore, in this research paper, it was emphasized that the resources of the company should be taken into account since the funds they could allocate for the ISMS may vary. It was also highlighted that the key risk in information security would be tied to the company's attitude towards it. Smaller companies may feel that they are not a target, and hence, may not feel the necessity to protect themselves. However, by making the ISMS understandable and clear, it can influence these companies to implement some of the controls, even without having a dedicated IT department or specialist. It was also stressed that even if the company is not working directly with patients, but rather providing tools for them, they would still handle the data of medical professionals, which should be secured.

In conclusion, this thesis has provided an overview of the documents and controls that were used to develop the ISMS for a small aesthetic medicine company. The ISO 27001 controls were used to develop the ISMS and address the company's weaknesses in information security. By developing the ISMS, the possibility of implementing it, taking into account the ISO 27001 standard, is high. The aim of this thesis was to secure the aesthetic medicine company with ISO 27001 by developing a suitable ISMS to address the risks they face. All the research questions were answered, and the findings of this thesis can be useful for other small companies facing similar challenges in information security.

5.1 Future work

Future research could be directed towards the implementation of an ISMS in a small aesthetic medicine company with a similar structure. Through implementation, it would become clearer which controls are more important than others, as effectiveness or ineffectiveness can be measured. In addition, the financial possibilities of the company and external competition could be considered to further refine the ISMS.

One potential area for future research is to investigate the impact of ISO 27001 certification on the aesthetic medicine industry. This could include examining the market demand for certified companies, the potential cost savings or revenue generation associated with certification, and the competitive advantages of being ISO 27001 certified. Another area of research could focus on the sustainability of the ISMS over time, including how it adapts to changes in the company's structure, technologies, and external environment.

Overall, the implementation of an ISMS in a small aesthetic medicine company is a continuous process that requires ongoing evaluation and improvement. By continuing to research and refine the implementation of ISMS, companies can better protect their assets and ensure the security of clients and business data.

References

[1] R. Southwick, "Cyberattacks in healthcare surged last year, and 2022 could be even worse", Chief Healthcare Executive, 2022. [Online]. Available: https://www.chiefhealthcareexecutive.com/view/cyberattacks-in-healthcare-surged-lastyear-and-2022-could-be-even-worse. [Accessed: 20- February- 2023].

[2] A. Furneaux, "Small to Mid Sized Businesses: How to Consider the NIST Framework", Cybersaint.io, 2022. [Online]. Available: https://www.cybersaint.io/blog/small-business-nist. [Accessed: 24- February- 2023].

[3] Mobayed, Nisreen, et al. “Minimally Invasive Facial Cosmetic Procedures for the Millennial Aesthetic Patient.” Journal of Drugs in Dermatology, vol. 19, no. 1, 1 Dec. 2019, pp. 100–103, https://doi.org/10.36849/jdd.2020.4641. [Accessed 25 -February-2023].

[4] Prendergast, P.M. and Shiffman, M.A. (2011). Aesthetic Medicine: Art and Techniques. [online] Google Books. Springer Science & Business Media. Available at: https://books.google.ee/books?hl=en&lr=&id=_yL0jc8DVsIC&oi=fnd&pg=PR3&dq=aesthetic+medicine+regulation&ots=TQSSOq_VAe&sig=jkjB-aG2JI1aSSH_pJfIsxz0_M8&redir_esc=y#v=onepage&q=aesthetic%20medicine%20regulation&f=false [Accessed 7-March-2023]

[5] ["ISO/IEC 27001 International Information Security Standard published". bsigroup.com. BSI. [Accessed 10-March-2023]

[6] Bird, Katie. "NEW VERSION OF ISO/IEC 27001 TO BETTER TACKLE IT SECURITY RISKS". iso.org. ISO. [Accessed 10-March-2023]

[7] ISO/IEC. "ISO/IEC 27001:2022". ISO.org. [Accessed 10-March-2023]

[8] Akinyemi, Iretioluwa; Schatz, Daniel; Bashroush, Rabih (2020). "SWOT analysis of information security management system ISO 27001". International Journal of Services Operations and Informatics. ISSN 1741-539X.

[9] "Facts and figures". bsigroup.com. [Accessed 10-March-2023]

[10]https://www.abebooks.com/9781516888429/Information-Security-Management-Based-ISO-1516888421/plp. “Information Security Management Based on ISO 27001: 2013: Do-It-Yourself and Get-Certified” Rafiandi, Andi; Radianis, Anis

[11] Whitman, Michael E, and Herbert J Mattord. Principles of Information Security. 6th ed., Boston, Mass., Cengage Learning, 2018.

[12] "What are Security Controls?". www.ibm.com. [Accessed 10-March-2023]

[13] Information technology — Security techniques — Information security management systems — Requirements Technologies de l'information — Techniques de sécurité — Systèmes de gestion de sécurité de l'information — Exigences. First (2005-10-15). Geneva: ISO/CEI. [Accessed 10-March-2023]

[14]ISO. (2022). ISO/IEC 27001 Standard – Information Security Management Systems. [online] Available at: https://www.iso.org/standard/27001 [Accessed 10-March-2023]

[15] (2020) The ISO 27001 Certification. https://www.researchgate.net/publication/347464114_The_ISO_27001_Certification

[16] ISO/IEC 17021

[17] ISO/IEC 27006.

[18] PECB. (2021). ISO 27001:2013 Information Security Management System - Requirements Whitepaper. [online] Available at: https://pecb.com/pdf/whitepapers/pecb-whitepaper_iso-27001.pdf [Accessed 10-March-2023]

[19] Technologies de l'information--techniques de sécurité--code de bonne pratique pour le management de la sécurité de l'information = information technology - security techniques - code of practice for information security controls. Second (2013). Geneva: ISO/CEI.

[20] Advisera Expert Solutions Ltd. “Checklist of Mandatory Documentation Required by ISO/IEC 27001” 2021. [Accessed 29-March-2023]

[21] Aleksejeva, Elina. “Samleks OÜ.” Samleks OÜ, www.samleks.ee/en/.[Accessed 10-April-2023]

[22] Kosutic, Dejan. “ISO 27001 Information Security Policy - How Detailed Should It Be?” Advisera.com, 26 May 2010, advisera.com/27001academy/blog/2010/05/26/information-security-policy-how-detailed-should-it-be/?utm_source=checklist-of-iso-27001-mandatory-documentation&utm_medium=downloaded-content&utm_content=lang-en&utm_campaign=free-blog-27001. [Accessed 10-April-2023]

[23] Dejan Kosutic “ISO 27001 Risk Management in Plain English” 2016. [Accessed 10-April-2023]

[24] NIST (2012). Guide for Conducting Risk Assessments NIST Special Publication 800-30 Revision 1 JOINT TASK FORCE TRANSFORMATION INITIATIVE. [online] Available at: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf. [Accessed 10-April-2023]

[25] Harris, S., & Herrmann, P. (2014). “Information security management handbook” sixth edition, volume 2. CRC press. [Accessed 10-April-2023]

[26] “Information Security Risk Assessment of dental clinic “Only Dent” 2022 Vugar Gafarli.

[27] Kosutic, D. (n.d.). ISO 27001 Asset Management: Develop an ISO 27001 asset register. [online] advisera.com. Available at: https://advisera.com/27001academy/knowledgebase/how-to-handle-asset-register-asset-inventory-according-to-iso-27001/?utm_source=checklist-of-iso-27001-mandatory-documentation&utm_medium=downloaded-content&utm_content=lang-en&utm_campaign=free-knowledgebase-27001. [Accessed 15-April-2023]

[28] Information technology -Security techniques -Code of practice for information security controls Technologies de l’information -Techniques de sécurité -Code de bonne

pratique pour le management de la sécurité de l'information. (2013). Available at: https://trofisecurity.com/assets/img/ISO-IEC_27002-.pdf.[Accessed 15-April-2023]

[29] Cichonski, P., Millar, T., Grance, T. and Scarfone, K. (2012). Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology. Computer Security Incident Handling Guide, [online] 2(2). doi:https://doi.org/10.6028/nist.sp.800-61r2. [Accessed 17-April-2023]

[30] Kosutic, D. (n.d.). Business Continuity Plan (BCP) Structure According to ISO 22301. [online] advisera.com. Available at: https://advisera.com/27001academy/knowledgebase/business-continuity-plan-how-to-structure-it-according-to-iso-22301/?utm_source=checklist-of-iso-27001-mandatory-documentation&utm_medium=downloaded-content&utm_content=lang-en&utm_campaign=free-knowledgebase-27001 [Accessed 20 Apr. 2023].

[31] Kosutic, D. (n.d.). ISO 27001 Internal Audit - Checklist, Explanations, & Guidance. [online] advisera.com. Available at: https://advisera.com/27001academy/knowledgebase/how-to-make-an-internal-audit-checklist-for-iso-27001-iso-22301/?utm_source=checklist-of-iso-27001-mandatory-documentation&utm_medium=downloaded-content&utm_content=lang-en&utm_campaign=free-knowledgebase-27001 [Accessed 20 Apr. 2023].

[32] International Organization for Standardization. 2013. "ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements." Geneva, Switzerland: ISO. [Accessed 20 Apr. 2023]

Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I Kristiina Šamanina

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis “Securing Aesthetic Medicine Company Samleks OÜ by the ISO 27001 Standard”, supervised by Valdo Praust.
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

11.05.2023

[1] The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.