ISMS Implementation and Maintenance in Compliance with Finland's National Cybersecurity Requirements

Svetlana Kim

Haaga-Helia University of Applied Sciences

Bachelor's Thesis

2022

Bachelor of Business Administration

Abstract

Author(s)
Svetlana Kim

Degree
Bachelor of Business Administration

Report/thesis title
ISMS Implementation and Maintenance in Compliance with Finland's National Cybersecurity Requirements

Number of pages and appendix pages
81 + 12

The thesis is dedicated to the research of common information security standards, regulations, and frameworks with the focus on Information Security Management System (ISMS) implementation and maintenance in compliance with the security requirements laid out on international and national levels.

The theoretical part includes research on development and operation of ISMS and presents an overview of the international and national cybersecurity requirements frameworks and regulations.

The empirical part is comprised by the comparative analysis of the international ISO/IEC 27002:2022 standard on information security and Katakri 2020 information security audit tool published by the National Security Authority of Finland. It also proposes a strategic approach to enhancing an existing ISMS with the purpose of reaching compliance with additional security requirements.

The research has revealed a strong common baseline security benchmark for information systems sustained by both ISO/IEC 27002 and Katakri with some differences in approach, focus areas, and individual controls. The work also reflects the developments in the information security field in comparison to the older publications.

The results can be used by organisations who want to improve their ISMS and reach compliance with new regulations, as well as anyone interested in gaining knowledge about management of information security and familiarizing themselves with common requirements, standards, and industry best practices.

Keywords
ISMS, cyber security, information security, cyber risk management

Table of Contents

Key Terminology

This section presents a brief explanation of a few concepts fundamental to the research. Provided explanations are consistent with the definitions set by the International Organisation of Standardization (ISO 2022a) and International Electronical Commission (IEC 2022).

The full list of the abbreviations used in the thesis is provided in Appendix 1.

Audit – systematic, independent, and documented process of obtaining and objectively evaluating the audit evidence to determine to which extent the audit criteria are fulfilled.

Business continuity plan (BCP) – documented procedures providing guidance on how to respond to a disruption, and resume, recover, and restore to a pre-defined operation level.

Compliance – fulfilment of a specified requirement.

Corrective action – action eliminating the cause of a nonconformity and preventing its recurrence.

Deficiency / nonconformity – failure to fulfil a requirement, inadequate implementation of the security controls.

Information Security Management System (ISMS) – part of the overall management system based on risk approach, designed to establish, implement, operate, monitor, review, maintain, and improve information security.

Information Security and Risk Management (ISRM) – coordinated activities aimed at directing and controlling organisation with regard to information risk and security.

Requirement – provision containing criteria to be fulfilled; need or expectation, stated, generally implied, or obligatory.

Security control - management, operational, and technical measures prescribed for an IT-system to protect confidentiality, integrity, and availability of the system and information.

Vulnerability – weakness in the asset, IT-system, security procedure, control, or implementation that can be exploited or triggered by a threat.

1 Introduction

The thesis presents an analytical review and actionable insights for the companies that want to ensure their compliance with the requirements of the cybersecurity regulations effective in Finland. Cybersecurity legislation and baseline business requirements are rapidly evolving, with the process often triggered by the recent precedents. This defines the need for strategic approach to improving organisations' security. There are guidelines and established best practises for Information Security Management System (ISMS) implementation based on the international standards. However, many organisations struggle with meeting the strict requirements dictated by their business sector or country of operation. Digitalization and information security professionals working in Finland face these challenges on the regular, and this project is meant to study and address these issues.

Research methods

The scientific methods applied in this project are mainly constituted by the qualitative research based on content and comparative analysis of the relevant legal documentation and literature sources. The applied tools include common cybersecurity frameworks and IT audit tools.

Set goals and objectives

The key objectives set for this project include:

- collecting and analysing the theoretical basis for the cybersecurity strategy development, ISMS maintenance throughout its lifecycle, and cyber risk management
- examining the commonly applied national and international cybersecurity standards and frameworks
- conducting comparative analysis of the international cybersecurity standards against the national Katakri 2020 criteria
- proposing a strategic approach to implementing the changes necessary to reach compliance with the Finland's national regulations for an existing ISMS.

Learning objectives

This work is also aimed at developing professional competences and getting comprehensive knowledge in the field of information security management. Adequate governance strategy is a decisive factor for implementing a functional security and risk management system. Understanding the governance aspect of security is the foundation for building a successful career as a specialist in the IT security field.

The set learning objectives are:

- solidifying knowledge about ISMS purpose, functions, governance, and operation
- getting more profound knowledge of international IT security standards and requirements
- studying Finland's national cybersecurity practices
- improving general understanding of information and cyber security.

Project Scope

Security requirements presented by the standards and regulations that do not apply directly to the cyber assets, for instance, technical requirements to physical barriers, locks, and emergency recovery systems, though are mentioned briefly in the overview, are outside the scope of this project. In addition, secure software development, including secure coding, testing, and production, are encompassed by the requirements, but do not comprise the focus of this work. This project also does not present exhaustive requirements for the industry-specific environments. Financial and healthcare systems are used as particular examples due to processing personal and other highly sensitive data as part of their operational needs. However, industry-specific regulations are a topic that needs to be explored separately per industry of interest.

Thesis structure

The thesis structure includes five chapters. Chapter 1, Introduction, describes the general idea of the project and its relevancy, outlines the thesis structure, and poses the goals and objectives for the work.

The second chapter explores the key concepts in cybersecurity focusing on security risk management and how ISMS helps to manage and mitigate the risks. It also describes the ISMS components, benefits, and lifecycle, starting with planning the implementation and throughout its operation, and the challenges connected with the implementation.

The third chapter discusses the differences between a cybersecurity standard, regulation, and framework. The overview of the specific standards, regulations, and frameworks commonly applied on the international and national level is also presented in this chapter. In addition, it discusses the importance of the IT systems' compliance and assessment based on the requirements criteria to ensure secure operation and get competitive market benefits of the security certifications.

The fourth chapter focuses on the comparative analysis between the ISO/IEC 27001 and ISO/IEC 27002 international standards' requirements and the criteria of Katakri 2020, a national security audit framework, with the goal of developing a strategic approach to reaching compliance with Finland's national cybersecurity requirements for organisations with an existing ISO/IEC 27001-compliant ISMS.

In the discussion chapter, the general results of the research are summarized, and the conclusions are drawn. The results have a potential for practical application in businesses on the national scale.

The abbreviations and respective explanations are given in Appendix 1. Appendix 2 provides an overview of the ISO/IEC 27000 series standards. Appendices 3 and 4 contain the lists of ISO/IEC 27002:2022 and Katakri 2020 requirements respectively.

2 Concepts of ISMS and Information Security Strategy

An Information Security Management System (ISMS) helps organisations to address and treat accordingly the risks related to information and information technology. According to the ISO/IEC standards (ISO/IEC 27000:2018, 11-12), an ISMS is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an organisation's information security to achieve business objectives. Implementing and running an ISMS is normally a part of organisation's information security strategy.

The modern commonly accepted stance on the information security strategy and its development is taking the risk-based approach as the core of the whole process. This means that the strategy starts with and is developed around the identified risks, risk assessment, risk acceptance, and risk management (Chopra & Chaudhary 2020). This is reflected by the combined term Information Security and Risk Management (ISRM) strategy, which will be used interchangeably with information security strategy in this work with the purpose of highlighting the central role of risk management in information security and encompassing both concepts within a unified process. In addition, section 2.2 of this chapter is dedicated to cybersecurity risk management, focusing on the procedures involved in the risk assessment and treatment.

The ISRM strategy provides the organisation with a defined action plan, including goals and objectives for protecting the organisational data and assets, and the necessary instruments to achieve these goals and objectives. The protection methods are chosen as part of the ISRM strategy taking into account the business goals and risks of a particular organisation. This chapter looks into the details of ISRM strategy development and risk factors, core elements, roles, and phases of an ISMS lifecycle, and the most significant factors affecting the successful functioning of the implemented system.

2.1 Organisation's Information Security Strategy

Security of data and integrity of operations are the crucial elements supporting and ensuring the business data staying safe and all business processes running smoothly. Information protection in an organisation is often seen as a purely IT personnel responsibility. With this approach, the development, implementation, and activities outlined in the ISRM strategy fall under the domain of IT department. The issues caused by this approach can include lack of understanding and exclusion of the processes run in the other business units, inability to influence the situation in the organisation and apply leverage to decisions made at the managerial level, and lack of proper financial support and other resourcing.

The industry best practices recommend starting and running information security transformation from the top, involving the top management in the development and introduction of the company's Information Security Strategy. The involvement and active participation of the personnel across business units is also important as it allows to naturally incorporate the established practices and support their improvement, as well as adapt the strategy to fit the needs of a particular business.

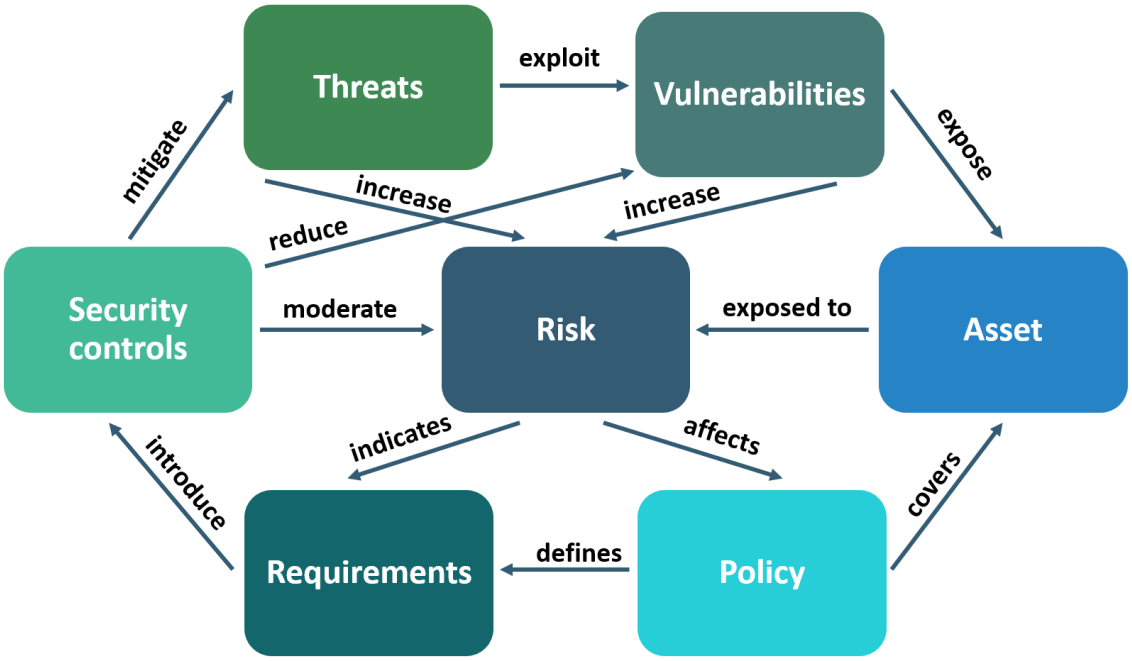

Figure 1. Connections between ISRM Strategy Components

As depicted in figure 1, ISRM strategy encompasses policies, security requirements, security controls, risk and threat analysis, vulnerability management, and asset management as a system of interconnected components. These components will be discussed in more detail in the following sections.

2.2 Cybersecurity Risk Management

As mentioned earlier, the information security strategy is built on the data analysis of the identified risks and risk acceptance. This information is collected and analysed by the information security department and delivered in the form of a risk analysis summary (presented on figure 2). When exploring the risks, the provision of information security cannot be separated from the goals, operations, and risks of the particular business (Chopra & Chaudhary 2020). The ISRM strategy is meant to be implemented in a manner that encompasses the risk map and integrates the maximum amount of business processes. In other words, it has to be optimized to fit the organisation.

Organisation Y: Risk Analysis Report					
Risk ID	Description	Likelihood	Consequence	Grade	Risk Owner
1.1	User account leaked	Possible	Mild	Medium	IT Helpdesk
1.2	Admin account leaked	Possible	Very significant	High	IT Helpdesk
2.1	Network: open ports	Unlikely	Significant	Medium	CISO Office
3.1	Server room: unauthorized access	Unlikely	Significant	Medium	Security
3.2	Server room: fire caused by electrical fault	Rare	Very significant	High	Maintenance
3.3	Server room: failure of power supply	Unlikely	Medium	Medium	Maintenace

Figure 2. Risk Evaluation Example

Risk analysis can normally be scenario-based (analysing possible events) or asset-based (carrying out assessment of each identified asset). Relevant scenarios, threats, and vulnerabilities can be identified by going through checklists of the most common threats and exploits and dedicated libraries. Figure 2 is an example of a scenario-based risk analysis. Likelihood of risk can be assessed by evaluating history, trends, and frequency of the procedures related to the risk being performed and calculating probability. The consequences can be the result of the direct impact (for instance, financial loss coming from paying fines for not fulfilling legal or contractual obligations) or indirect impact (for instance, financial loss coming from reputational damage and losing customers). The grading is done in accordance with the risk heat map presented in figure 3. The risk heat map is a concept, and the scale can vary significantly between the organisations. (Alexander & al. 2013; Alan Calder 2019.)

	Consequence				
Likelihood	Insignificant	Mild	Moderate	Significant	Very significant
Rare	LOW	LOW	LOW	MEDIUM	HIGH
Unlikely	LOW	LOW	MEDIUM	MEDIUM	HIGH
Possible	LOW	MEDIUM	MEDIUM	HIGH	HIGH
Likely	MEDIUM	MEDIUM	HIGH	HIGH	VERY HIGH
Very likely	MEDIUM	MEDIUM	HIGH	VERY HIGH	VERY HIGH

Figure 3. Risk Heat Map Example

Low risks can be accepted and incorporated in the routines for periodic review. Moderate risks require responsibility assignment and treatment, including regular review. For high and very high risks immediate moderation is in order. The risk can be lowered by reducing likelihood and minimizing consequences. For very high risks, top management involvement in the development and approval of the treatment plan might be required.

The main purpose of cyber risk management is to identify risks related to information technology and develop measures to respond to them accordingly. ISO standard 31000 (ISO 31000:2018) on risk management defines risk as an effect of uncertainty on objectives.

ISO/IEC 27000 standard series comprising the basis of the research part in this work is a risk-based tool outlining information security management best practices. It is commonly used as a framework for assessing organisation's security posture. The requirements laid out in the standard help to evaluate and address the risks affecting organisational data. They can also be helpful in tracking the status of organisation's risk resilience. (Alan Calder 2019.)

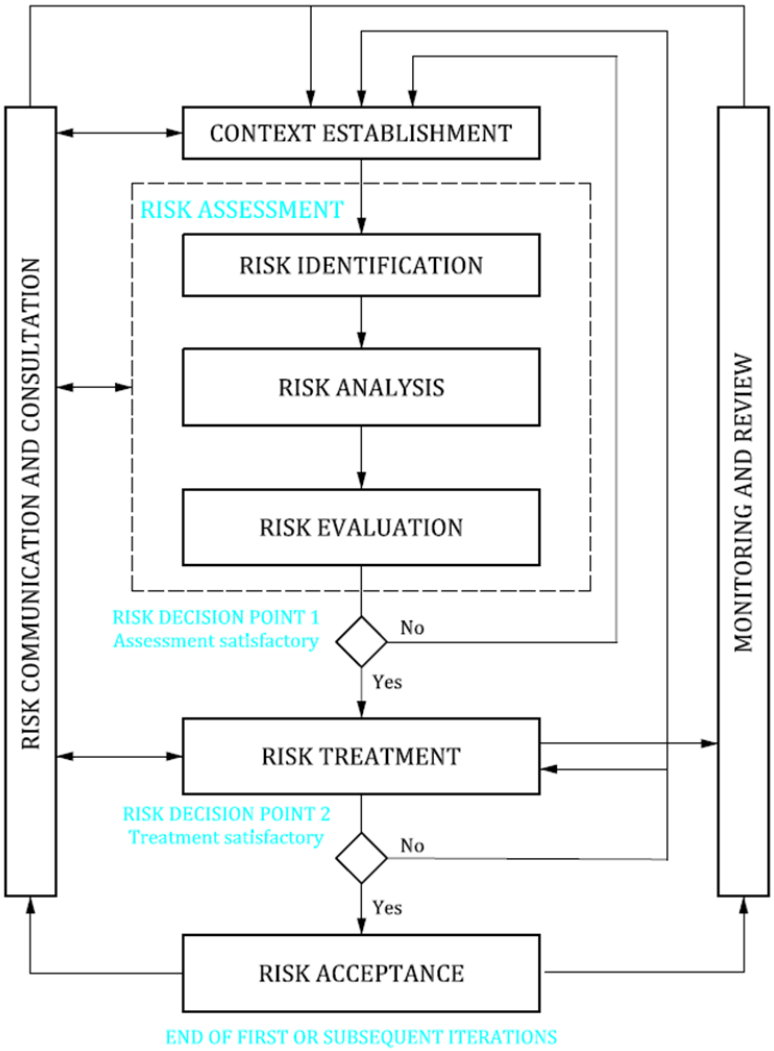

Figure 4. Information security risk management process (ISO/IEC 27005:2018, 4)

Information security risk management process defined by the ISO/IEC 27005 standard is presented in figure 4. ISO/IEC 27005 standard is an Information Security Risk Management standard giving guidelines on risk identification and analysis, evaluation and acceptance criteria, risk treatment, communication and consultation, monitoring, and review of risk factors.

Through risk analysis the organisation understands what risk levels are acceptable and can be mitigated, and what risk factors call for immediate action and elimination. Acceptable risk levels are also defined in the security standards and regulations. By fulfilling the standardized requirements, the organisation demonstrates that it is does not take unnecessary risks. (Chopra & Chaudhary 2020.)

Once the risks are identified and mitigation actions are outlined, the continual improvement stage starts. At this stage, the organisation reduces the risk levels by adopting respective company policies, providing accessible guidance for the employees, and introducing necessary changes to the operations. Risk monitoring is performed through the regular testing and control. This can be done in the form of the operator functions i.e., regular check tasks for the designated employees, as well as more formal verification during the internal and external audit. Continuous identification and assessment of the possible new risks is part of the process. Emerging risks can be associated with the changing situation on the market, need for changes to the implemented technologies and established processes, new technologies adopted by the company or subcontractors involved in the business operations, newly discovered or arising IT threats.

2.3 Purpose and Structure of ISMS

The main purpose of ISMS can be defined as safeguarding business continuity and security of data. This purpose encompasses a number of objectives, such as minimizing risk, protecting data, and limiting the area of effect in case of a security breach.

ISMS addresses protection of organisation’s information from unauthorized disclosure, modification, or loss of access, also known as the CIA (confidentiality, integrity, availability) triad, a guiding model in information security. As defined by the International Organisation for Standardization, confidentiality is a property that information is not made available or disclosed to unauthorized individuals, entities, or processes, integrity is a property of accuracy and completeness of information, and availability is a property of being accessible and usable on demand by an authorized entity (ISO/IEC 27000:2018, 2).

As discussed in the previous section, the ISMS framework normally builds on the risk assessment and risk management. It can follow common criteria for the security standards or focus on industry- and organisation-specific risks. The security controls, as well as the implementation methods, are chosen by the organisation based on the context of the organisation, industry sector, and the results of the risk analysis.

2.3.1 Standard Components of ISMS

The ISMS components can vary significantly depending on the organisation. In addition to the previously discussed systematic approach to information security, ISO/IEC standards (ISO/IEC 27000:2018, 11) also define an ISMS as a system consisting of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organisation, in the pursuit of protecting its information assets. There is no universal solution, and each system needs to be developed and optimized for the adopting organisation's needs. However, some common elements can be outlined.

Information security governance category covers information security policies, business continuity planning (BCP), incident management, change management, distinction of roles and segregation of duties, and information classification. It addresses the threats and risks within organisation's IT systems and networks, such as external and internal threats, system failures, and data loss. Information security policies provide general direction and specific operational guidelines. The policies are company-specific, which means they are planned in accordance with the business line and organisational needs. BCP ensures continuous operation of the business and aims to prevent, or at least minimize, service interruptions. It also details the recovery action plans for incident recovery, minimizing the damage caused if an incident does happen (Alexander, Finch, Sutton & Taylor 2013). One of the most important BCP-related matters is Data Loss Prevention (DLP), which deals with safeguarding and preserving organisational data through data backup and redundancy of facilities. Incident management is aimed at identifying and resolving IT issues, minimizing the impact on the operations and system's end users. Change management deals with planned changes to the system, such as regular and emergency updates, upgrades, IT systems retirement and migration to the new IT systems, and access rights changes. Roles and responsibilities also need to be clearly defined and documented, ensuring all tasks have a responsible owner, and no operations are being overlooked. This is also strongly connected with the access rights management and just enough access, which is discussed in more details in the next paragraph. Information classification allows the organisation to assign their data assets to a specific category, usually associated with the respective protection levels. Protection level guidelines laid out by the government provide instructions on how a specific information category is supposed to be processed

and secured. Proper governance ensures compliance with the security requirements imposed by the government authorities for the respective business sector. (Patel 28 March 2021.)

Identity and access management (IAM) category deals with identification, authentication, and authorization of users. Initial identification implies that when the user first registers and get access to the system (for example, as part of the employment), their identity is verified and associated with an identifiable individual. This can be done through a face-to-face meeting with an ID card check, but a commonly used and governmentally approved method in Finland is strong authentication with banking credentials involving MFA. Authentication requires the user to prove their claimed identity every time they log into the system. Multi-factor authentication (MFA), and two-factor authentication (2FA) at minimum, is considered to be the security standard. Authorization defines which resources and functionalities of the system the authenticated user can access and utilize. It also promotes one of the key principles of modern cybersecurity – the principle of least privilege. The principle of least privilege means that the employees and subcontractors only get access to the information that they need to perform their immediate duties (just enough access) and only for the time when they need it. It's important to note here that user accounts with elevated access rights (e.g., IT administrators) often have standing privileged access to the system, which is currently shifting to just-in-time access, when privileged access rights are only granted for a limited predefined time when they are needed. This is considered more secure in case of a cyber-attack because it prevents the attacker from utilizing privileged-level actions even if they are able to get a hold of an admin account. (Chopra & Chaudhary 2020.)

People processes handle all the aspects concerning individuals involved in the business operations and getting access to organisation's data and systems. This involves screening or security clearances for the personnel upon recruitment, raising information security awareness and related trainings, confidentiality agreements or NDAs for the internal employees and subcontractors, chain of command for reporting security incidents, policies for secure distant working and BYOD (Bring Your Own Device) if the employees are allowed to work remotely and use their personal devices for work-related purposes (Patel 28 March 2021). Contractual relationships with subcontractors and third-party suppliers should be aligned with the security policies, as external employees might need to access the network or organisational data. It is not always possible to enforce the internal information security policies for these relationships. In order to mitigate the potential risks special controls and contractual obligations have to be in place. People controls also involve internal HR processes, such as start and end of the employment or change of position within the company. Associated system changes (transferring information to IT about the

need of change in access rights), issued and returned devices, onboarding and exit procedures fall under this category.

Assets management covers organisation's assets including equipment, devices, and information assets. A detailed inventory of assets should be maintained with the turnover planned out and documented. Information system acquisition, development, and maintenance are closely connected to the change management as well, because security best practices need to be maintained and controlled throughout the entire lifecycle (Patel 28 March 2021). Technological assets and data disposal are some of the main aspects of assets management. For instance, certified e-waste recycling entities can be contracted for secure storage media disposal and automation can be used for timely data disposal.

Operations and communications management implies the integration of policies and controls in the system's operation, meaning that daily IT operations should follow IT security guidelines and ISMS controls (Patel 28 March 2021). For example, encryption methods used for data both in transit and at rest should use adequate modern encryption methods, such as AES algorithm for transferring highly sensitive data, and comply with the cryptographic controls outlined in the regulations. Cryptography, active protection against malware on workstations (AV), system and traffic monitoring to detect anomalies, inbound traffic filtering, logging of user and admin activities, network segmentation and isolation are all methods to protect the system enabling secure operation and communication.

Physical security guidelines regulate actions aimed at protecting premises and physical assets, including IT equipment, from damage, loss, and unauthorized access. Some key security requirements can include physical barriers and locks preventing unauthorized access to the facilities and equipment; entrances, servers, and operating rooms being illuminated and monitored by the security personnel, as well as recorded via camera surveillance; screen filters used when working in an open office; cables protected from interception and damage, including power, data transfer, and other IT support cabling; protection against espionage and eavesdropping. In addition, there are requirements for emergency remediation and recovery. These requirements include redundancy of data storage media, for instance, data servers duplicated to an isolated facility, possibly to a different physical location; fire alarms and flood protection; redundant UPS (Uninterruptible Power Supply) rooms and systems and emergency power supply generators. In Finland, Katakri, Subdivision F: Physical Security can be used to assess the facility's security (National Security Authority of Finland 2020). Nowadays many organisations choose the benefits of the cloud services, which allow them to put the responsibility of maintaining physical servers on the Cloud Service Provider. In this case, it is still customer's responsibility to find a suitable CSP (Cloud Service Provider), whose premises are compliant with the respective

regulations depending on the customer's sphere of operation. The specific security requirements applied to the cloud services are laid out in the PiTuKri assessment tool (Traficom 2020). Moreover, even if CSP's services are used to store organisational data, workstations and employees' personal devices used to access this data need to be checked for compliance with the security requirements and continuously monitored.

2.3.2 Key Roles and Responsibilities

Organisations have different structures and hierarchy, so the way cybersecurity specialists and activities are integrated within that system has to be decided based on the adopted business model. An example of the company structure diagram reflecting the roles from the ISMS point of view can be seen on figure 5.

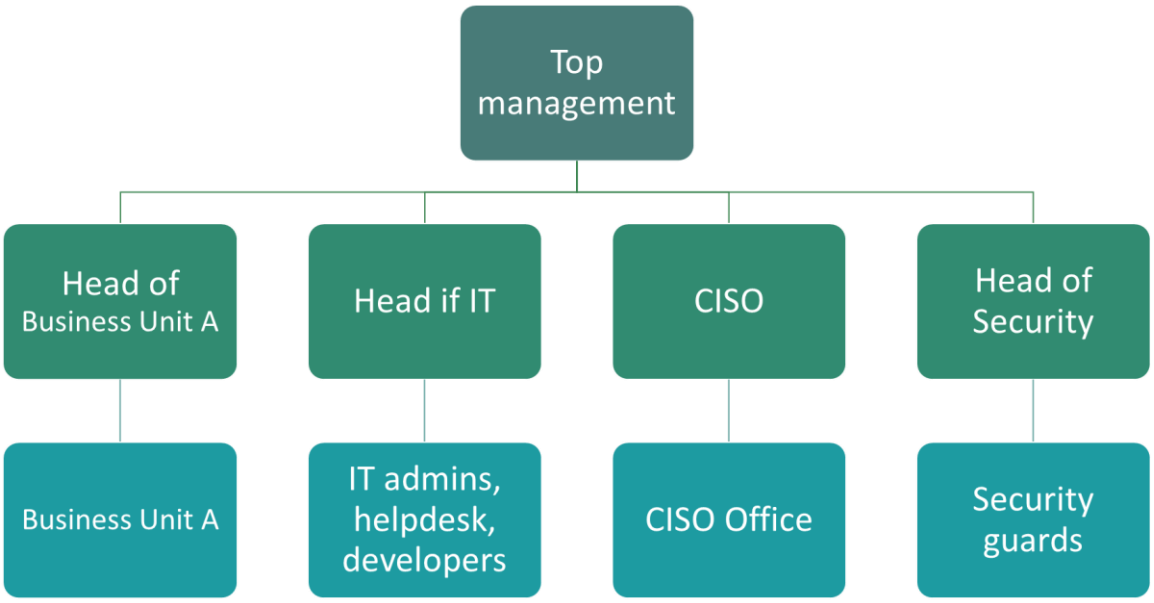

Figure 5. Example of a Company Structure Diagram Displaying ISMS-related roles

ISMS-related responsibilities include establishing, implementing, maintaining, monitoring performance, and improving ISMS; information security risk assessment and treatment; designing processes and systems; setting standards for configurations and operation of security controls; incident management; ISMS review and audit; documentation and reporting (ISO/IEC 27003:2018, 9).

Top management are responsible for setting general direction for the security activities, defining the ISRM strategy, approving policies and programmes, designating leaders, and establishing communication throughout the organisation. Top management does not need to assign all responsibilities but should delegate the authority to do it. The management also needs to ensure that the goals of the information security strategy are aligned with the general business strategy of the organisation. They are the ones allocating financial

budget and other resources for the ISMS-related activities, and taking decisions based on the information provided by the cybersecurity specialists and analysts. One of the most important decisions is setting the level of acceptable risk based on the monitoring of the changes in the threat field and identified risks. They are also ultimately responsible for ensuring that the established procedures are enforced, and the system is compliant with all the relevant legal and regulatory requirements. The results of the performed procedures are reported to the top management to support further decision-making and, consequently, business operation.

CISO (Chief Information Security Officer) coordinates all the information security-related activities and is the one in direct contact with the top management, reporting on the performance of ISMS and significant security events.

Information Security Department, led by CISO, holds a major responsibility for designing and developing a functioning ISMS. This includes identifying, planning, and implementing all the necessary layers of defensive technologies. They perform regular review of the monitoring reports and active system scans and are also the first to respond to a security event, deciding whether the detected anomaly or incident is a false alert, or if it requires triggering the response procedure, and escalation to the reporting chain.

The IT Department, depending on the organisation’s structure combined or separated from the Information Security Department, implements the necessary technological elements of ISMS, and maintains the ICT infrastructure. IT administrators are also normally the ones performing the IAM activities, controlling granting, revoking, and changes of the user rights.

Physical security, normally organised as a separate unit, should have the measures established as part of the information protection efforts embed in their routine duties. In bigger organisations that have, for instance, internal audit and analytics departments, there can also be additional roles, such as IT auditors conducting regular evaluation of ISMS performance, security analysts working specifically on risk identification, analysis, and developing mitigation strategies, and forensics specialists investigating the security events.

Employees are responsible for following guidelines applicable to their role in the organisation. They should understand their responsibilities and be held accountable for compliance with the set policies. Raising awareness through role-specific trainings ensures that employees recognise the need for security measures in place. In many organisations, there is also a binding clause in the employment contract requiring the employee to confirm that they have read through, understood, acknowledged, and agreed to act in accordance with

the Information Security Policy and other documents related to IT assets and data protection (e.g., device acceptable use policy, remote working, information classification), as well as an NDA. On top of that, the job description and procedures for the operations should have security-related activities and necessary safeguards imbed, so it is considered part of normal operation. Organisation's subcontractors are also required to comply with these policies, sometimes in adjusted capacity.

Information security activities include the entire organisation. Organisation's information security strategy can only be effective if everyone follows its guidelines, and one weak link is enough to start an intrusion, so its everyone's responsibility to support the ISMS in its operation. All business units need to be aware of their responsibilities and relevant threats to watch out for.

2.3.3 Benefits of ISMS Implementation

The fundamental benefit of ISMS is directly connected to one of its key purposes: an ISMS protects and enables the CIA triad for data and information technology within the business operations. It provides a framework for keeping organisational data safe and managing it centrally. The framework is constituted by policies, procedures, and controls aiming to protect the confidentiality, availability, and integrity of information. It secures and facilitates the management of information assets in all forms (e.g., paper-based, digitally stored, cloud stored, intellectual property, personal data, etc.).

It also increases the cyber-attack resilience, allowing to effectively respond to evolving security threats. It protects organisation across business units, not only through defensive technologies, but also through raising employees' awareness and involving security in business operations by design. Continual improvement approach supports introducing adjustments prompted by changes within the company, as well as in the external environment, reducing the threat of emerging risks.

The holistic approach means that the system encompasses the whole organisation, not only the IT department. This promotes the improvement of company culture, enabling employees to understand risks and involve security controls as part of their everyday working practices (Dutton 4 June 2019). A robust ISMS enables organisation to establish and protect their reputation of a trustworthy employer, business partner, and service provider.

A thoroughly designed ISMS can help an organisation in complying with regulations and winning the market. One of the major benefits from the business perspective is that an ISMS helps to protect business and customer data, which is essential to consolidate the

company's position on the market and gain customer trust. Customers will often require the organisation to prove their trustworthiness and credibility before entering into a contractual agreement. This becomes crucial in the sectors where highly sensitive data is processed, for instance, financial and healthcare sector. In many countries, specifically in the EU, the requirements for the companies processing personal data are set at the legislation level and are mandatory to comply with before the business can start operation. This is where the cybersecurity certifications come into effect. There is a variety of certifications based on the regulations and standards applicable per and across business sectors locally and internationally. Some are referenced by the legislation and approved by the authorities, others are widely accepted and considered the standard industry practice. Specific information security regulations, standards, and frameworks, as well as the importance of the organisation's information security posture assessment, are discussed in detail in Chapter 3.

An ISMS also facilitates compliance with the regulatory, legal, and contractual obligations, helping to avoid breaches and associated complications. ISMS controls clearly identify relevant requirements, ISMS procedures provide actionable guidance for business processes and possible scenarios, automation and reminders facilitate the execution of regular tasks, and documentation keeps the information about the system updated and ready for use when needed. This complex of measures ensures that both daily operations and exceptional cases are handled in accordance with the law, commercial agreements, and best security practices. (Schou, Faber, Hernandez, & Slay 2014.)

Finally, the expenditures coming from information security are reduced in the long run. Initial development and implementation of an ISMS can be expensive, with additional costs coming from audit and certifications if those need to be obtained. However, risk assessment and analysis allow to optimize operations and avoid spending time and resources on ineffective layers of defensive technology. Moreover, information security governance is necessary to avoid fines imposed by the authorities. For example, according to the General Data Protection Regulation (GDPR) organisations can face fines of up to 10 million euros, or 2% of their global annual revenue, whichever amount is higher, for smaller infringements. For more severe infringements, the fines are up to 20 million euros, or 4% of global annual revenue, whichever is higher (Wolford s.a.-a). The biggest fine was received by Amazon in July 2021 amounting to 746 million euros. And in January 2022 Google Ireland and Google LLC were imposed a fine of combined 150 million euros (Sullivan 18 March 2022).

2.3.4 Common Challenges of ISMS Implementation

Considering all the practical benefits of an ISMS, it is an essential part of a modern business structure. Nevertheless, it is important to keep in mind the potential complications that might come to light when an ISMS is developed and adopted and think through the ways of overcoming these challenges upfront.

One of the main challenges and the first step in developing the system is risk assessment, which has already been discussed in detail earlier in this chapter. Risk assessment is a critical stage and the basis of an ISMS implementation. During this stage, a register of information assets is compiled, risks are identified, analysed, and evaluated. The risk assessment methodology should include organisation's security requirements, risk scale, and justified acceptable risk level. The common risk assessment challenge is that it seems very complicated and time-consuming due to its complex and all-encompassing nature (Jucan 5 September 2022). However, it can be streamlined to a straightforward process of assessing the risk against the CIA of the affected information by scoring the severity of consequence (event affecting the objectives) and multiplying it by the likelihood (chance of the event happening) to determine the final risk score. When mitigating actions are taken and confirmed to reduce the severity or likelihood, the risk is re-evaluated, and the risk level is lowered. (Mooney 2015, 58-59.)

Scoping the project correctly can be difficult. It is important to understand that the ISMS does not need to cover the entire organisation from the beginning. This is especially relevant for larger enterprises. Usually, it makes the most sense to start small, focusing on the IT systems that are involved with the customer services. This is the area that will pose the most interest for the clients and authorities. Subsequently, after the general framework has been developed and part of the organisation was assessed in the first cycle, other parts of the organisation, like HR systems, can be gradually included, along with the newly added services. (Sharron 2022.)

System documentation is another key component of an ISMS. Many organisations struggle with producing initial documentation and consequently maintaining it up to date, because this involves recording all the operations and assets across the organisation. In addition, documentation has to be done in accordance with the standards (Jucan 5 September 2022). It is an extensive project that usually involves multiple task owners including representatives of all departments. However, it is crucial to allocate the necessary time and resources, because in crisis situations this is where you can find the directions and references to the required information. When it comes to the HR turnover, documentation

is needed for the induction of new employees, giving them an understanding of the procedures and systems in place, as well as to prevent the fundamental knowledge leaving the company when an employee who participated in the development and implementation of the ISMS terminates their employment. This is also the primary way to show the authorities, the auditors, and the customers that the organisation complies with the legislation, protects customer information, and simply does the right thing in terms of security of their operation in general.

During the initial phase of developing an ISMS, an organisation should conduct gap analysis to get the general understanding of the policies, procedures, and systems that are already established and functioning, as well as to identify the parts that are missing and need to be built from the ground up. This can be a complex task requiring concise planning. In order for it to be efficient it is vital to keep all the relevant stakeholders included in the conversation. For instance, in case some documentation has already been created but is not available as a shared material, or some automated process is already implemented but lacks documentation. It would be a waste of time and resources to recreate these elements, so it's important to have the people on board who know exactly what the status of the module in question is.

Effective communication during the ISMS implementation can be a challenge itself. It is vital to document the process and update all the stakeholders accordingly. It is helpful to agree at the start of the project what communication channels will be used to discuss the matters at hand, what tools will be used for collaboration, and what storage media will be used for file sharing. Keeping employees informed also makes people more invested in the project and interested in its outcome, as they can see direct connection with their work, and can provide valuable input for the project.

Understanding the requirements of the standard or regulation that an organisation strives to comply with also causes difficulties for the project team (Jucan 5 September 2022). It is a common practice to hire an external consultant or take on board a new employee for curating the project. A cybersecurity specialist with vast industry experience and expertise in ISMS, who has already worked with similar ISMS implementation and assessment projects before, provides qualified contribution and a fresh view on the internal procedures that might cause issues.

Finally, budgeting the project and allocating the necessary human, time, and financial resources is a challenge that can be in the way of the success of the project. Therefore, it's imperative that the top management understands the critical role of cybersecurity, being

supportive of the project and willing to invest in its successful implementation. (Sharron 2022.)

2.4 ISMS Lifecycle

The common approach to an ISMS project is quite similar to many other IT projects: the process is divided into a number of sequential phases. The fundamental phases that can be formally identified are planning, development, implementation, maintenance, and continual improvement. Each phase can include smaller composing stages or tasks. The phases and tasks can also be re-iterated multiple times as needed when the system expands and incorporates newly identified risks, additional systems, or business units. (Kosutic s.a.)

The phased project approach allows the team to follow a number of steps with clearly outlined tasks, making the whole process manageable and less daunting. Employees responsible for the development and implementation of the ISMS in the organisation can focus on performing specific tasks with defined deliverables and reporting.

2.4.1 Planning

ISMS implementation and support is an extensive and continuous project spanning over several years and it needs to be planned out carefully. It usually requires both long-term and short-term planning. Long-term strategic management plan covers the period from 1 to 5 years (usually 3-5 years, depending on the target certification), giving strategic direction to the process, and outlining high-level goals. A corresponding short-term operational plan (up to 1 year) contains technical tasks and specifications for the immediate actions. It is revised regularly (at least annually), as some of the tasks get completed and objectives are updated. The final goals in the long-term plan remain fixed, while the short-term plan gets adjusted to reflect the changes in the business state providing flexibility and efficiency. The organisation is also enabled to keep track of the changes in the current situation and forecast its needs in the field of cybersecurity for the future. The plans set clear goals and make them achievable by breaking them down into manageable and adaptable tasks. (Kosutic s.a.)

The scope of the project is defined during the planning phase. Larger organisations can start implementing ISMS covering one part of organisation or certain business processes, which significantly lowers the project risk and the effort required to succeed in the implementation. Specifically, the customer services should be included, as they will be the focus of the business operations. As organisation’s information security matures, other processes and business units can be gradually included. For a smaller company, it is easier

to include the entire company in the scope, and then upgrade the system as the business grows.

Assuming that all the resources in the organisation are already in place and functioning as expected, it would still take at least a couple of years to develop the ISRM strategy and the ISMS based on it, implement them, and get the target certification. A certification's standard validity period is usually 3-5 years, and it needs to be renewed after that. Annual internal and external audits are conducted in the interim, to keep the information up to date, verify that no changes have been made that would significantly shift the security state, identify new potential risks, and perform regular checks mandated by the organisation's security policies and procedures.

The first year is usually the most intense in terms of workload, as this is when a major part of development, implementation, and preparation for the first inspections happens. Capital and operating expenses are also at their highest during the first year of the implementation, but by the second year they stabilize and start going in line with the changes. The short-term plan for this period should clearly define what is to be done, who is responsible for each task, and what are the deadlines. Standard project management tools such as Gantt chart and Kanban board can be used to visualize the assignments and progress.

The plan also describes in detail the desired state of the system and the business after the project, specifically the internal organisational processes and the security posture. The best way to determine what the project aims to achieve is to work directly with the senior management to understand the goals and expectations of the top managers. (Chopra & Chaudhary 2020.)

2.4.2 Development

After the project is initiated and planned out with the support of the management, the development of the ISMS starts. As already discussed, risk analysis and the resulting ISRM strategy are the starting point and the building foundation of an ISMS. Risk assessment methodology defines the rules for identifying risks, assessing their impact and likelihood, and establishes acceptable risk level (Alan Calder 2019). Once the ISRM strategy is in place and the ISMS goals are laid out, it is necessary to collect information across organisation for the gap analysis that would accurately describe the current state of the business and information security and compare it against the set targets. The gap analysis should reflect which policies, procedures, processes, systems, and other elements of ISMS are already in place and effective, which ones need to be reworked or adjusted, and which ones need to be developed from scratch.

An Information Security Policy needs to be developed as the ruling internal document defining baseline requirements for the organisation's information security. It does not to be very detailed, since other unit- and system-specific documentation will provide the necessary operational guidelines. Information Security Policy gives general guidelines on secure work practices and handling information and explains how these guidelines are controlled.

After the risk assessment is complete and the Information Security Policy is ready, the organisation should have a thorough understanding which security controls are applicable. The relevant controls can be found, for example, in the national regulations, or international standards, such as the Common Criteria for Information Technology Security Evaluation (CC) and ISO/IEC 27001 Annex A. These standards and regulations are reviewed in Chapter 3. The organisation can follow one of the standardized control frameworks adapting it to their own needs or create a unique control framework adapting it to comply with the sought certification requirements. The special document, Statement of Applicability (SoA), is created listing all the controls and specifying which are applicable and which are not relevant in the context of the specific organisation. For the applicable controls the chosen implementation methods are described. For the controls that are deemed not applicable, the reasoning for this decision is provided along with a reference to the compensating controls if such controls exist.

The Risk Treatment Plan is another risk-related document that needs to be written at this phase. It gives details on how exactly the controls outlined in the SoA will be implemented, including the assigned personnel, timelines, and budgeting. In other words, it is a controls-focused implementation plan used to coordinate the project. Risk treatment can follow one of the following strategies:

- Retention (acceptance): the risk is deemed necessary, but not significant enough to take immediate action. Periodic monitoring is needed.
- Reduction: the risk level is lowered by eliminating some of the risk factors, reducing the likelihood or impact.
- Transfer: the risk is transferred to the service provider, for example, through getting an insurance, or outsourcing part of the activities.
- Avoidance: the risks with high likelihood and impact must be eliminated entirely.

Finally, the measure of the controls' effectiveness needs to be established for all the security processes. The control environment needs to be assessed appropriately with security metrics. It is also important to remember that the controls do not dictate the implementation or how the business should be operated. Security must be integrated in the business

operations, but the security controls can be compensated with other controls as long as they provide equal protection level to the resources in question. Internal and external audits produce the report on the effectiveness of the controls' implementation. If some nonconformities are discovered during the audit, the correction plan is developed addressing the issues, and corrective actions are taken to fix the nonconformity or mitigate the risk through other methods. (Chopra & Chaudhary 2020.)

2.4.3 Implementation

The implementation phase starts with risk treatment performed in accordance with the developed Risk Treatment Plan applied against the risks identified during the risk analysis. The purpose of risk treatment is reducing the necessary risks' levels to the acceptable state and eliminating the risks that can be eliminated or cannot be accepted. After that, the Risk Assessment Report is updated to reflect the new reduced risk levels, steps taken during the risk treatment process, and documented approvals of the residual risks by the authorized party.

Implementation of the security controls is a major part of the implementation. At this step, all the planned-out security procedures, technologies, and adjustments are brought into practice. It involves creating all the necessary automation, regular tasks, installing physical barriers, such as locks, safes, screen protectors, installing supplementary IT tools, such as monitoring software and AVs, and enforcing new standards. The specifics of implementation will depend on the controls that the organisation is adopting in their control framework. (Chopra & Chaudhary 2020.)

New practices can face some resistance from the employees who are used to perform their duties in a certain manner. Besides that, the awareness of information security and the associated threats can be rather low. It can be raised through implementation of training programs. The trainings can involve courses, videos, tests, seminars, practices, and other arrangements covering the organisation's Information Security Policy, general security guidelines, and role-specific trainings relevant to the employee's position. Where relevant, the trainings should cover secure operations, information access, software use, device use, communications, incident reporting, information classification, and remote work. For the employees to stick to the directives, they need to have an understanding of the importance of cybersecurity and why these procedures are necessary to safeguard the business and its data. (Mooney 2015, 103.)

2.4.4 Operation and Maintenance

Once all the processes, security technology layers, and other ISMS elements are implemented, the actual ISMS operation starts, and the system needs to be maintained and optimized. The directions for ISMS operation can be found in the governance documentation along with the task owners responsible for the specific operations. It is vital to ensure that the organisation performs all the activities described in the policies and procedures, complies with the prescribed requirements, and produces factual records. If the documented procedures prove to be overly complicated in practical application, they should be reworked in order to be manageable and better reflect the hands-on experiences of the process operators. ISMS becomes an integral part of organisation's daily routine and there are several principal focus areas.

To begin with, it is important to monitor and measure the ISMS. The developed efficiency metrics should help with this task. The goal is to measure whether the ISMS achieves the intended results. As such, the practical results are checked against the objectives set in the planning documentation. If there is a mismatch, it means corrective and preventive actions have to be taken. Corrective actions should be systematic, meaning that the root cause is identified and resolved, and successful remediation is verified. It is a beneficial learning opportunity to prevent future possible incidents. (Kosutic 14 July 2014.)

On top of that, the information security specialists should be aware of the current state of ISMS, for instance, how many and what type of incidents happen, are there some atypical behaviours, do the automated processes function properly with no interruptions, are there any system failures, how IT resources are utilized by the employees. All the security-related events, such as incidents, errors, and exceptions, need to be closely monitored. In addition, it is vital to keep records on all the relevant activities to facilitate monitoring and audit, identify and analyse anomalies in a timely manner, and have the evidence materials available for investigation in case of a security incident.

Management review is a basic operation control method. The managers do not need to be involved in the controls' implementation, but they need to be aware of the ISMS-related activities in order to make informed decisions promoting information security in the organisation through aligning security and business strategy, budgeting, and administrative actions. Moreover, additional approvals of the authorized personnel are a common security measure for the ISMS-controlled procedures, such as risk management and acceptance, change management, incident management, and disciplinary actions. It provides an extra layer of security and an independent, qualified counsel on the actions taken. (Kosutic 14 July 2014.)

Regular management reviews are conducted on monthly, bi-annual, or annual basis, depending on the frequency of the control or procedure being run. During the regular review, the manager inspects the documentation and evidence produced by the subordinate business unit and issues a statement on the correctness of the records. A good example of such review would be an access rights review performed bi-annually by the IT department manager. As part of the procedure, all the user records are verified, and any discrepancies are fixed after investigation of the root cause and appropriate treatment.

A business is a dynamic structure, meaning the external and internal circumstances, state of technology, active IT assets, potential risks, and many other factors will frequently change. All the ISMS-related documentation must be regularly updated in accordance with these changes to reflect the actual state of the business. Regular documentation review should be conducted by the management at least annually. Upon this review, the technical documentation is revised and updated, policies and procedures are adjusted, and the components that are no longer deemed relevant are abolished. Documentation update is also covered by the change management procedure. A common practice is to have a document or service owner responsible for the update tasks for each system or business unit.

Risk assessment is another component that would require regular updates. As threats and vulnerabilities are altering, associated risks are changing, and the controls derived from these risks need to evolve as well in order to keep the risks manageable. To support this, the results of the risk assessment are transferred to the risk owners for regular review and update. The risk owners also provide suggestions on mitigating risks and implementing new controls when deemed necessary.

Internal audit, also called first-party audit, can help with controlling the ISMS operation. Internal audit might reveal security vulnerabilities that were not exposed previously. For instance, employees might not be aware that they are performing some of the operations in a way that goes against security guidelines and standard procedures. The goal is to identify such cases and take corrective measures to prevent the issue from recurring. The internal audit team is built from the professionals that are knowledgeable about the audited systems and processes but maintain independence from the audited activities, not running the controls in question directly. In other words, a person should not audit their own work. A lot of companies choose to hire an external auditor for this purpose, while bigger enterprises can have a whole QA (quality assurance) and internal audit department. Before the audit, the team must familiarize themselves with the audit methodology and relevant controls, and develop the audit procedures, unless those were established previously. The

audit procedures cover the documentation and evidence to inspect, sample sizes, processes performed by the operators, and technologies to test. Internal audit also helps to prepare and practice for the external audit that is conducted for the certification assessment. The more thorough the internal audit procedures are, the easier it will be for the organisation to pass the assessment and obtain the sought certification: the interviewees know what sort of questions to expect, the relevant evidence is at hand, and the system for collecting and storing the evidence is well-organised. (Chopra & Chaudhary 2020.)

External audit can be conducted as a second-party audit, for example, by the stakeholders and clients, or as a third-party audit, conducted by the independent assessment body usually with the purpose of obtaining certification. When it comes to the third-party audit, the first year is crucial, as this is when most of the system assessment is performed, and the initial decision is drafted on the compliance with the requirements. If some major deficiencies are found, the corrections plan is developed, and re-assessment needs be held. If there are only minor nonconformities, the certification is granted. After the certification is obtained, the certification body performs surveillance visits at least once a year, testing efficiency of the controls and whether deficiencies identified the previous year were fixed (Chopra & Chaudhary 2020). The external audit is discussed in more detail in Chapters 3 and 4 in relation to the IT-security certifications that organisations might want to pursue.

2.4.5 Continual Improvement

It is crucial not only to maintain the ISMS functioning, but also to improve its quality, optimize it for innate integration in business operations, update it to match the rapidly changing business context, revise and adjust the parts that do not function properly, and expand the coverage including more parts of the business. ISO/IEC defines continual improvement as a recurring activity to enhance performance (ISO/IEC 27000:2018, 2). ISMS implementation should be designed to promote and support the organisation’s digital transformation by adapting to the ongoing advancement and improvement of the security policies and controls. The scope and structure of an ISMS might also be relevant for a limited time only. As the company’s service offering, resources, culture, business context, risks, and other factors evolve, so should the associated security control mechanisms.

The PDCA (Plan-Do-Check-Act) cycle is a common management tool for control and continual improvement. It is often applied in IT-systems management and iterative design of digital services. However, this approach is not exclusive to the ICT field. Rather, it is a generalized framework that can be applied to any type of product or service. ISO 9001 Quality Management Systems standard and ISO/IEC 27001 Information Security Management standard require to implement methods for continual improvement of the systems.

The ISO 9001 process model is based on the PDCA cycle, as this principle is applicable to various processes (Abuhav 2014). There are no direct requirements posed by the standards for which method specifically should be used, but PDCA cycle is promoted as the preferred method for most IT security teams.

As it can be seen from the figure 6, PDCA is a dynamic iterative four-step model. PDCA can be applied to all changes in the organisation, in this case, changes to the IT security policies and procedures, layers of technology, systems, communications, or awareness trainings. Overall, it involves planning, implementation, control, and continual improvement. Regardless of what sort of change is required, the basic four steps highlighted by the name remain the same: plan, do, check, act. When applying this model to ISMS processes, it's makes sense to consider each step in the context of IT security controls.

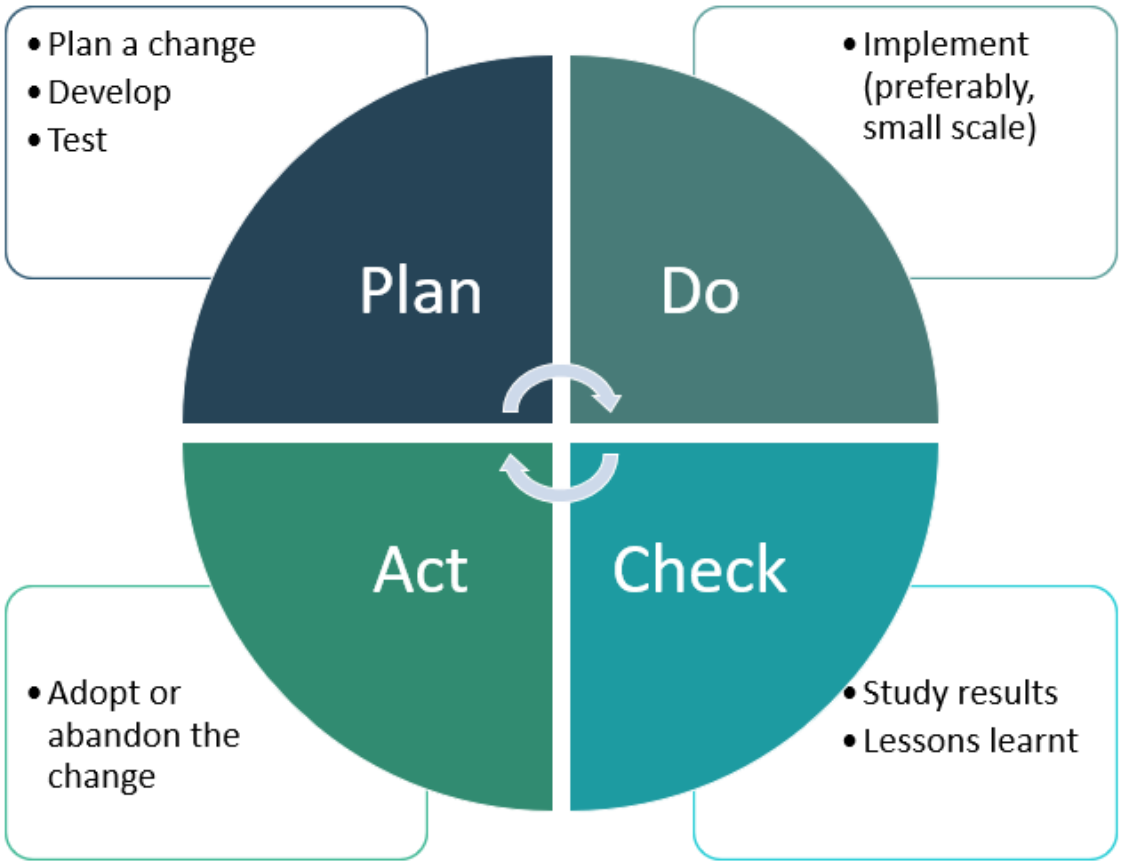

Figure 6. PDCA Cycle (adapted from Van Otterloo 2017)

Plan: the planning step answers what, when, where, and by whom needs to be done. First, the processes or systems that need improvement are identified. Before starting the implementation of the changes, the activity is planned out. The team needs to think through which ISMS element is being improved, what are the possible ways to improve it, what is the end goal, and how the effectiveness of the change can be measured. The resources are allocated, the timeline is defined, and the current state is documented. To control the cost and effectiveness of the proposed solution, key performance indicators

(KPIs) are developed. The metrics used for KPI assessment can vary depending on the organisation and changes in question, the only expectation here is that it is relevant and aligned with the ISMS goals. For instance, it can be reducing the number of security incidents, raising the completion percentage for the employee awareness training, or minimizing the number of manual operations.

Do: at the doing step, all the planned activities are performed. For example, installing a new system monitoring tool, creating a task with an automated notification for all employees in the company's intranet, or developing and enabling new automated workflows. This step is basically the testing phase of the cycle.

Check: also known as Study, implies monitoring and measuring the processes and comparing the actual results against the planned objectives and requirements. After the changes have been implemented, the effectiveness of the change should be evaluated by analysing the collected metrics. Some changes will not be as effective as planned, and others might even worsen the KPIs. In this case, the root cause of the issue is investigated, discovered, analysed, and eliminated. For example, if an organisation comes up with a large number of security controls completely restructuring their technology layers, and instructs the IT department to prioritize this restructuring, it might overload the capacity and interfere with normal operations. On top of that, if all the upgrades and changes are pushed onto the systems at once, it will most likely disrupt the services and halt all the business processes altogether. Either way, the findings have to be documented and reported so that further actions can be taken based on the gathered information. The data obtained during this step is also useful to identify other affiliated inefficiencies and opportunities for improvement.

Act: also known as Adjust, at this step the results obtained from the Check step define which measures are adopted for improving the performance. If the changes were successful, they are made permanent. For example, automation scripts go from testing to production environment. Documentation should also be updated to reflect the changes. Otherwise, the correction plans are developed, and the cycle continues. It is also useful to collect feedback from all the stakeholders in order to gain some valuable insights for the future PDCA iterations of ISMS controls and elements. (Abuhav 2014.)

2.5 Additional Considerations

There are also some affiliated factors significantly affecting the effectiveness of information security strategy and ISMS implementation that are not directly addressed by the standards and regulations but are still essential to take into account. These factors are not

technology- or ISMS governance-related, however, they can be a decisive factor for the success of the project. Rather than being strict requirements, these considerations come from the experience of the organisations and professionals who have already run these projects and had to deal with these lateral issues. The insights gained from these experiences can be categorized under the umbrella term “best practices”. Some of the best practices for ISMS implementation are shortly addressed in this section.

First of all, when initiating the ISMS implementation project, the fundamental understanding of the current state of the business and cyber security is essential. When developing ISRM strategy, the information security goals must be aligned with the business goals. If an organisation lacks staffing, budget, or interest in building a robust and secure by design system, the ISRM strategy should honestly reflect and address this situation. It is always better to find appropriate risk mitigation methods for these risk points already in the development stage, than see the project fail at a later stage, when considerable amount of time and resources have already been invested. For instance, if the company lacks appropriate expertise, a CISO with experience in similar projects can be hired to lead the development and implementation, or an external agency’s consultancy can be secured to guide and curate the process. If the company lacks financial resources, the initial implementation can be scaled down with the imbed flexibility allowing the system to scale up gradually as the business grows. If some of the employees or top management believe that cyber security is immaterial, and think that an ISMS would be redundant, it’s important to hold an awareness campaign explaining in accessible terms and figures why keeping the organisation’s data and processes protected is vital for the business to prosper, or survive at all, in the modern business environment. It is vital to gain support of the stakeholders, so that people involved in the process feel enthusiastic about their contribution and recognize that it makes a difference. (Sharron 2022.)

The financial state is one of the key indicators of the current business situation. If there is a negative trend, it might be best for the information security department leaders to downsize or even postpone the implementation of the large-scale changes to focus on supporting current business requirements and facilitate organisation getting to a healthier state financially. If the organisation is experiencing growth in the financial performance, this is likely the best time to implement a robust ISMS, which would further increase the value of the business. In addition, when the business is expanding, the potential cyber-attack surface increases and new risk points emerge, which means there are more processes, data, and systems to be protected.

It is also necessary to understand project budgeting and its structure. Organisation’s revenue for the financial year has to be taken into account when allocating the budget for a

specific area, such as cyber security projects. Of course, the budget evaluation for an ISMS project does not need to be impeccably accurate, this is the goal that is challenging to achieve with any project. However, the managers leading the project need to be realistic, not to underestimate largely the required resources, and not to overpromise, setting grand goals on a tight budget. A common fallacy is thinking that the most important thing is initiating the project, assuming that additional funding can be requested and obtained later on. This might lead to the project running out of budget earlier than any tangible results could be achieved, effectively wasting time and whichever funds were allocated in the first place, along with discouraging everyone involved from continuing to work on the improvements of organisation's information security. It is better to set small, attainable goals, feasible in terms of budget, and take on more ambitious enhancements once the organisation can afford it. Of course, the ISRM strategy should not be completely dependent on the budget, and the long-term ISMS plan should aim for better security over any other considerations. While security goals are fundamental, reasonable budgeting shows that the project leaders understand the business and have clear vision of the work required, which will help to obtain top management support. (Kosutic s.a.)

Allocating human resources and giving employees sufficient time to work on the project is another crucial planning aspect. The resources that the company has, specifically intangible resources, such as employee expertise, will determine organisation's ability to execute the developed strategy in accordance with the determined timeline. The personnel issue is one of the major concerns, as the organisation might end up in a situation when they have an elaborated strategy and plan, sufficient funding, but no staff to perform the work. The staffing requirements are especially high during the implementation stage as the workload is significantly higher than during the regular operation and maintenance. The organisation can consider hiring temporary, part-time, or independent consultant personnel to build up their workforce for those limited high intensity periods. IT department might also need more human resources as new systems, layers of technology, automations, or other IT-related assets are introduced as part of ISMS. The current personnel might not have the required knowledge about the new technologies, or simply be overloaded with the amount of maintenance and support that needs to be done for these new assets. The existing people resources need to be correctly assessed during the ISMS development phase, recognizing which expertise is missing, and the necessary personnel has to be recruited. (Sharron 2022.)

Finally, the existing company culture should be taken into consideration. Knowing and understanding the company culture becomes pivotal when introducing the new Information Security Policy and other guidelines. The governance parts of ISMS should be adapted to the company culture, allowing for security by design and seamless integration of security

practises in all the operations whenever possible. General information security awareness should also be raised and maintained. All the employees need to understand why the specific procedures exist and why it is beneficial to follow them. ISMS can only be effective if all the people affected by it support the system and stick to the guidelines. If an organisation has democratic culture and employees can openly share concerns and ideas, the most effective way for the IT security leaders to introduce the ISMS would be involving all the stakeholders from the beginning of the planning phase, including the strategy discussion, and achieve consensus on all the major decisions. In organisations with more bureaucratic culture based on directives from the top management strictly followed by the employees, open discussion would not produce the same results. In this case, it is vital to gain the support of the top managers, pitching the idea and possibly several implementation options. In addition, elaborating specific, clear, and detailed instructions forwarded by the managers to all the employees would be the most effective way of enforcing security practices. In either case, regular and active communication between the top management, the project team leaders and members, and the affected employees is necessary.

The best practices facilitate effective ISMS implementation and operation. This is possible thanks to the IT security standards leaving space for flexibility. Strictly following a certain standard and trying to implement all the controls does not guarantee instant evident improvement of organisation’s security posture. An organisation can choose whichever methods fit their needs, goals, budget, IT personnel, and culture, as long as they provide adequate protection level to the data and processes.

3 Cybersecurity Standards, Regulations, and Frameworks

This chapter presents an overview of some requirements commonly applied to IT security and ISMS both in Finland and internationally. Prior to looking into specific approaches to IT security, it is necessary to understand the terminological difference for the concepts of cybersecurity frameworks, standards, and regulations.

A framework is the most general term out of the three. A cybersecurity framework is a tool for developing a system that would be comprehensive in covering all the relevant assets, optimized to the organisation's unique business case, and compliant with the applicable requirements. It is an implementation guidance based on the established standards and practices aimed at reducing cyber risks levels. When talking about the specific requirements of the regulations or standards, like ISO/IEC 27001 Annex A, professionals will often use the term "control framework" to describe the list of laid-out requirements and associated controls, meaning the structure that the organisation would need to implement and subsequently audit in order to reach and verify their compliance.

Cybersecurity standards establish the baseline of security for IT systems. Standards are voluntary to follow and are usually established by the private institutions aimed at protecting the information technology environments by collecting best practices, tools, policies, and procedures for reducing risks and proving layered defence mechanisms. The most widely accepted industry standard for information security is ISO/IEC 27000 family (including requirements specified in ISO/IEC 27001 Annex A).

Unlike standards, regulations are developed by the governmental institutions to support law enforcement, and therefore are mandatory to comply with. Regulations are normally applicable on a national level. There are several industry-specific regulations in Finland applied to the systems operated by financial, healthcare, and governmental organisations, mostly on the grounds of processing citizens' personal data. Regulations give clear directives on what level of protection the implemented security measures should provide. These directives are referred to by laws, and an organisation might face substantial fines if they are not implemented as prescribed. (Wright 2008.)

3.1 International Cybersecurity Requirements

Starting with the international cybersecurity practices, this section gives an overview of the ISO/IEC 27000 family, ISO/IEC 15408 Common Criteria for Information Technology Security Evaluation, GDPR, and NIST CSF. There are many other cyber security frameworks,

such as OWASP Foundation's Top 10 presenting most common security issues in applications and services often used for IT services security evaluation, or PCI DSS (Payment Card Industry Data Security Standard) developed by a coalition of bank card service providers (Visa, MasterCard, American Express, Discover, and JCB), which the companies that handle online and other card payments and store card holders' data must comply with (Kirvan & Granneman 2021). A few popular control frameworks are mostly followed by the American organisations and are enforced by the USA governmental entities e.g., SOC2 used by the service organisations, mainly in financial sector, to assess their systems against the AICPA TSC, HIPAA used by healthcare organisations to secure personal healthcare data in electronic format, and FISMA used by federal agencies to protect governmental systems (Mutune 2019). The ones reviewed in this section are the most relevant for this research due to outlining ISMS-specific requirements and being widely spread worldwide.

3.1.1 ISO/IEC 27000 Series

ISO/IEC 27000 series is a family of standards developed by ISO (the International Organisation for Standardization) and IEC (the International Electrotechnical Commission). The series present a collection of guidelines on information security and cybersecurity management best practices built around the governing ISMS. The series have a broad scope, encompassing IT security, privacy, confidentiality, governance, awareness, and other IT-related issues.

There is a total of about 50 standards. The number of standards is constantly changing, as new standards get developed and published, while old standards are withdrawn or replaced with updated versions. The complete and accurate list of currently effective standards can be found in the catalogue published on the official ISO website. (ISO 2022b). The list includes:

- vocabulary standard (ISO/IEC 27000, "Information security management systems – Overview and vocabulary")
- requirement standards (the main one being ISO/IEC 27001, "Information security management systems – Requirements")
- general guidelines (e.g., ISO/IEC 27003, "Information security management systems – Guidance", and ISO/IEC 27007, "Guidelines for information security management systems auditing")
- sector-specific guidelines (e.g., ISO/IEC 27011, "Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organisations", and ISO/IEC 27019, "Information security controls for the energy utility industry")

- control area-specific guidelines (e.g., ISO/IEC 27033, “Network security”, and ISO/IEC 27035, “Information security incident management”)
- extensions to standards (e.g., ISO/IEC 27701, “Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines”).

Figure 7 presents a visualised structure of the ISMS standards series.

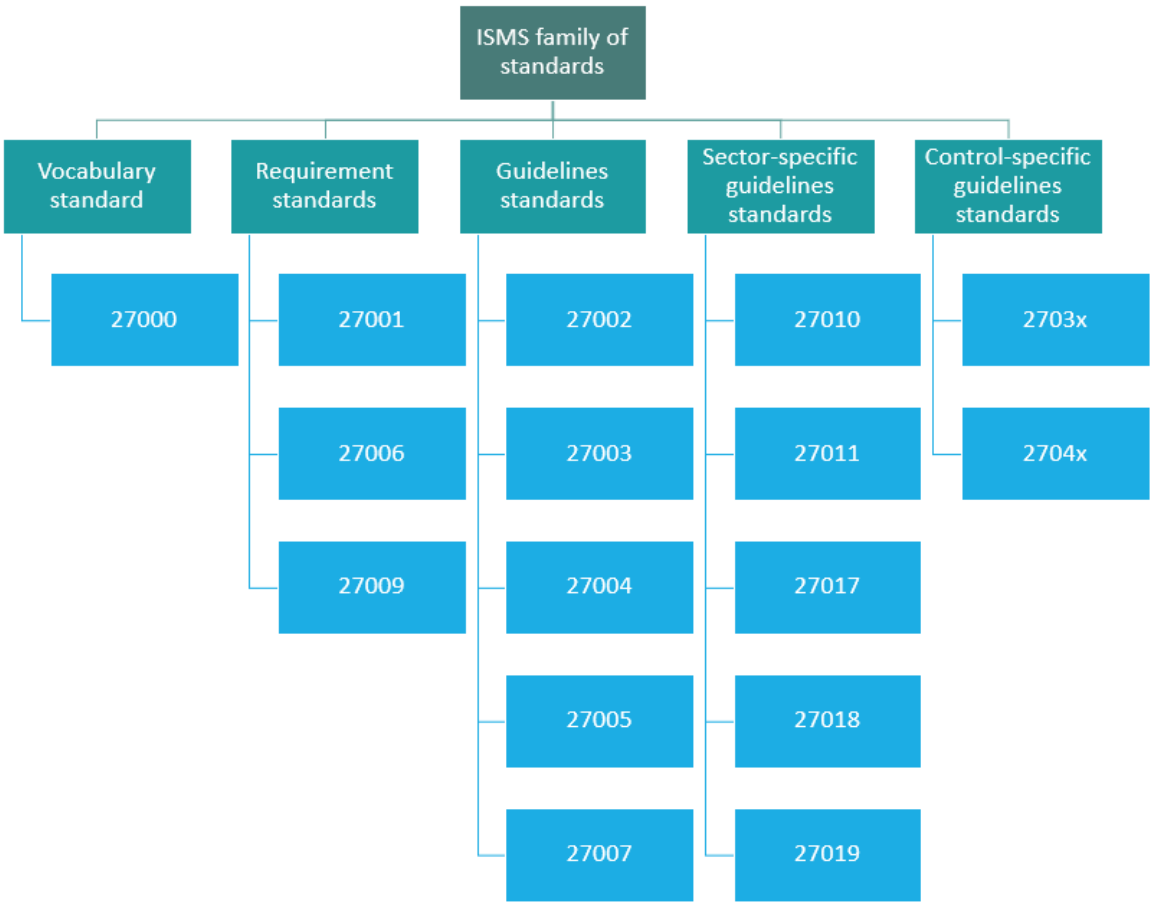

Figure 7. ISMS Family of Standards Structure (adapted from ISO/IEC 27000:2018, 19)

The primary standards give security requirements and controls for organisations to comply with, but do not dictate the specific methods of implementation. Guidelines and codes of practice give implementation examples and specifications for the requirements, which an organisation might choose to follow. In addition, organisations are encouraged to identify, analyse, and treat the information risks. Specifically, the standard ISO/IEC 27005 on Information security risk management addresses approach to identification of the relevant assets, threats, and vulnerabilities, risk analysis methodology, assessment of consequences (impact) and likelihood, risk level evaluation, risk treatment, and risk acceptance criteria (ISO/IEC 27005:2018). In the context of this research, it is most important to look at the first five documents in the series directly related to ISMS (ISO/IEC 27000-27004).

ISO/IEC 27000, “Information technology – Security techniques – Information security management systems – Overview and vocabulary”, is an introduction to the whole series. The latest version was published in 2018 and it is the fifth edition of the standard. It gives a description of the whole ISMS family of standards, including scope and purpose of some of the key standards, clarifies the verbal expressions used in the documents, and provides definitions for the key terms commonly used in the standards. To ensure terminological consistency, all the standards in the family rely on the terms and definitions provided by ISO/IEC 27000. The standard also covers the topics of ISMS and management systems, information security, ISMS lifecycle, and benefits of ISMS standards series. (ISO/IEC 27000:2018.)

ISO/IEC 27001, “Information technology – Security techniques – Information security management systems – Requirements”, is the central overarching information security standard outlining ISMS requirements. The latest version of the standard was published in 2013. The standard is built around risk assessment and ISMS. It gives specifications on establishing, implementing, operating, monitoring, reviewing, maintaining, and improving ISMS in the context of organisation’s business risks. The purpose of this standard is providing normative requirements for development and operation of an ISMS based on a set of controls for mitigating the risks associated with the information assets that the organisation aims to protect. It specifies the implementation requirements for information security controls adapted to organisation’s individual needs. The controls and respective definitions are given in the Annex A of the standard. The complete framework is comprised by 114 controls. ISO/IEC 27001 is the only certification standard in the series, meaning that organisations can be formally assessed against it and achieve compliance certification. Most of the other standards provide specifications, implementation examples, and expansions for the requirements listed in ISO/IEC 27001. Organisations are only required to implement those controls from Annex A that are deemed relevant based on the sector and risk analysis. For this purpose, an SoA (Statement of Applicability) document is prepared by the organisation, listing the applicable controls and their implementation, and providing justification for the controls that were declared non-applicable and excluded from the control framework. When implemented, the controls help to mitigate the identified information security risks. The requirements presented in Clauses 4-10 of the standard are mandatory for compliance with no permissible exceptions. (ISO/IEC 27001:2018.)

ISO/IEC 27002, “Information security, cybersecurity and privacy protection – Information security controls”. The previously used version of this document was published in 2013. The newest third edition is already published and is planned to come into effect in July 2022. The standard provides guidance on implementation of the information security controls in compliance with the requirements listed in ISO/IEC 27001 Annex A. In other

words, the content is similar to ISO/IEC 27001 Annex A, but each control is accompanied by an additional “Implementation Guidance” section. ISO/IEC 27002 presents a comprehensive overview of each control, explaining how it operates, how it can be implemented, and what are the objectives. It lists some commonly accepted control objectives and best practices in implementation that can be used as a guidance when deciding on the relevant controls and implementing them. ISO/IEC 27002 groups controls into four categories:

1. Organisational (such as information security policies, roles, and responsibilities, reporting to the authorities and stakeholders, inventory of assets, information classification, access control, identity management, supplier relationships, incident management, IT-related BCP, privacy, and documentation)
2. People (such as security clearance, awareness, disciplinary process, HR-related procedures, NDAs, working remotely, and incident reporting)
3. Physical (such as premises security, securing facilities, physical security monitoring, protection against physical and environmental threats, working securely, security of equipment and assets, storage, supporting utilities, cabling, maintenance, and secure disposal of assets and equipment)
4. Technological (such as securing endpoints, privileged access rights, access restrictions, secure authentication, malware protection, vulnerabilities management, configuration management, data retention, backup, and disposal, redundancy of data and information processing facilities, logs, system monitoring, software installation, networks security and segregation, traffic filtering, encryption of data at rest and in transit, secure software development and system architecture, change management, and testing environments).

The purpose is to create an adequate, suitable, and effective ISMS providing assurance to stakeholders and keeping the IT infrastructure reasonably secured and protected against threats. (ISO/IEC 27002:2022.)

ISO/IEC 27003, “Information technology – Security techniques – Information security management systems – Guidance”. The second, most recent, edition of the guidance was published in 2017. The guidance gives clarifications and recommendations regarding some of the concepts and requirements presented in ISO/IEC 27001. Its purpose is providing background to the successful implementation of an ISMS through understanding organisation’s unique context and needs, determining the scope, aligning the information security strategy with the business strategy and leadership strategy. It also covers ISMS lifecycle, including planning and risk analysis, implementation, support, operation, performance evaluation, and improvement. (ISO/IEC 27003:2017.)

ISO/IEC 27004, “Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation”, the latest version, the

second edition, was published in 2016. The guidelines aim to assist in establishing procedures to evaluate effectiveness of the implemented controls and ISMS performance, and to continuously improve these procedures. They cover the monitoring and measurement criteria and the analysis of the obtained results, specifying what, when, by whom, and how should be measured, analysed, and evaluated. The main purpose of the document is providing a framework to assess the effectiveness of an ISMS and information security controls. (ISO/IEC 27004:2016.)

The full list of standards (currently published or being under development) from the ISO/IEC 27000 series can be found in the table attached in Appendix 2.

The defining feature of the series is its flexibility. The standards do not dictate what an organisation is supposed to look like. This allows for accommodation of organisations of all sizes from various business sectors and facilitates establishment of a system that would support their unique business needs. The difficulty comes from the fact that it is up to the organisation to define and set up the system in accordance with their business model. This means that coming up with the ways to implement the requirements falls under the responsibility of the organisation. The final goal is to demonstrate security and compliance of the system.

3.1.2 ISO/IEC 15408 (Common Criteria)

The Common Criteria for Information Technology Security Evaluation, usually referred to as just Common Criteria (CC), are used as the basis for the ISO/IEC 15408 standard. The standard defines guidelines for evaluation of security functionality of an IT system, service, or product against a common framework. CC standard was developed under the premise of being applicable with various National Schemes (cybersecurity regulations developed and effective on national level). The current version of the standard is 3.1 published in 2017.

CC is comprised by the 3 main parts and the supporting Common Evaluation Methodology document. Part 1, Introduction and General Model, gives an overview of the evaluation and directions for specifications of Security Targets and Protection Profiles. Security Functional Components listed in Part 2 are categorized in 11 classes: security audit, communications, cryptographic support, user data protection, identification and authentication, security management, privacy, protection of security functions, resource utilization, TOE (Target of Evaluation) Access, and Trusted Path. The Security Assurance Components listed in Part 3 are categorized in 10 classes: protection profile evaluation, security target evaluation, configuration management, delivery and operation, development, guidance

documentation, life cycle, tests, vulnerabilities assessment, and maintenance of assurance. Parts 2 and 3 are catalogues of the requirements to align the claims in the Security Target or Protection Profile with.

Security Target is the specifications of the product or system. It includes the overview, conformance claim, asset description, usage environment, security objectives and requirements, security functions, and assurance on how the requirements are met.

Protection Profile (PP) is the product type-specific security criteria, focusing on a category of security devices or software products (e.g., security tokens, firewalls). The product must comply with all the requirements outlined in the PP. Currently, there are 37 approved and internationally accepted profiles, including email clients, encrypted storages, operating systems, remote access, traffic monitoring, USB flash drives, VPNs, LANs, virtualization, and web browsers. New PPs are constantly being developed. Each Protection Profile covers product type or system family description, intended use cases and environment, associated threats, organisational security policies, security objectives, functional and assurance requirements, and rationale for the identified objectives and requirements.

The Common Evaluation Methodology (CEM) contains directives for the evaluators. The produced documentation and collected evidence should be detailed and technically sound. CEM explains the requirements defined in Part 3 and can be adapted as a control framework for evaluation. CC certification can be obtained by completing an evaluation for the relevant Protection Profile at the chosen Evaluation Assurance Level.

Evaluation Assurance Level (EAL) specifies the depth of the performed testing. There are 7 predetermined EALs in total, with 1 being basic and every consecutive one being more extensive. The EAL's grade reflects how many tests have been performed but does not necessarily directly correlate with the level of security of the IT product or system. The 7 levels are:

- EAL1: Functionally Tested. Verifies that the IT asset operates as intended and claimed in the documentation, meeting the specified requirements. This level can be applied when cyber threats are not considered significant.
- EAL2: Structurally Tested. Provides basic level of assurance. Can be applied for IT assets with limited developer access, for instance, legacy systems.
- EAL3: Methodically Tested and Checked. Verifies moderate level of security by thorough inspection and testing of the TOE and development process. Often applied for the OSs or similar complex IT assets.

- EAL4: Methodically Designed, Tested, and Reviewed. Provides high assurance level, often applied for products with security-specific engineered features (e.g., firewalls).
- EAL5: Semi-Formally Designed and Tested. Provides high level of assurance with independent security testing and verifies TOE's ability to withstand a potential attack. Usually applied when special level of security is crucial (e.g., smart cards).
- EAL6: Semi-Formally Verified Design and Tested. Provides assurance for high-value assets in high-risk environments with a formal model of security policies and semi-formal functional specification.
- EAL7: Formally Verified Design and Tested. Provides assurance for high-value assets in extremely high-risk environments. Only applied in special cases.

(Mead 2013.)

Common Criteria can be used not only for evaluation of an IT asset's security, but also for the system or product acquisition at the stage of creating an RFP (Request for Proposal). The profiles can be used to identify the requirements corresponding to the needs. It is also an effective tool for creating system documentation, product description, or an RFP response, as it can be used to define all the relevant features and components. Additionally, CC can be referred to when designing or developing IT security functionality in software, firmware, and hardware.

3.1.3 GDPR

The General Data Protection Regulation (GDPR) is the privacy and security law put into effect by the European Union on May 25th, 2018. The requirements of GDPR are imposed on all organisations worldwide that collect and process personal or other data related to the citizens of the EU. The Regulation is comprised by 11 chapters and a total of 99 articles, covering lawfulness and principles of personal data processing, categories of data, individual's rights, responsibilities of the data collector and processor, security of processing, supervising authorities, and other related issues.

Article 5 of GDPR outlines protection principles for processing of personal data. The processing must be lawful, fair, and transparent to the person whose data is processed. The purposes of processing should be explicitly declared when data is collected, and its usage should be strictly limited to these purposes. The principle of data minimisation means that data should only be collected in the capacity adequate and relevant to the purposes of processing. If the data is in the format that permits personal identification, it should only be stored for as long as necessary. The principle of accuracy requires data to be accurate and updated. The principle of integrity and confidentiality focuses on data security, access

restriction, retention, and protection against loss or damage. Finally, the accountability principle states that the data controller is held responsible for compliance with all these principles.

The Regulation recognizes individual's right to be informed about data collection in a transparent manner (Articles 12, 13, and 14); to access information regarding purposes, categories, scope, and period of data collection (Article 15); to data correction or erasure (Articles 16, 17, and 19); to restrict processing (Articles 18 and 19); to be provided a copy of the personal data undergoing processing (portability, Article 20); to object to processing (Article 21); and to not be subjected to automated decision making and profiling, with the exception of special circumstances (Article 22).

Article 25 promotes the protection of data by design and default, meaning that the organisations are required to implement appropriate technical and organisational measures for data protection, taking into account the context, scope, and risk analysis. It also refers to Article 42, Certification, pointing out that organisations can demonstrate compliance by getting an assessment and certification from an accredited certification body.

The requirements include, for example, restriction of unauthorized access to the stored data, least privilege principle, MFA enforcement, and end-to-end encryption. The goal is to ensure that the data is transferred, processed, and stored securely, and can only be accessed by authorized parties. It also gives additional control to the users over their personal data and how it is used. (Wolford s.a.-b.)

3.1.4 NIST Standards and CSF

NIST is an American National Institute of Standards and Technology. NIST has developed and published multiple standards, many of them focusing on IT security, and, notably, the Cybersecurity Framework (NIST CSF).

NIST SP (Special Publication) 800 series is a collection of IT security recommendations, guidelines, and annual reports on NIST's activities in this sphere. The publications' main goal is addressing the needs of Federal Government of the United States. Federal agencies are encouraged and, in some cases, required to comply with the NIST standards. The guidelines are widely adopted by the private sector organisations as well.

NIST SP 800-53, Security and Privacy Controls for Information Systems and Organisations, is a baseline security guideline for the American governmental institutions. The most

recent, fifth, edition was published in 2020 and includes the following control families: access control; awareness and training; audit and accountability; assessment, authorization, and monitoring; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; program management; personnel security; personally identifiable information processing and transparency, risk assessment, system and services acquisition, system and communications protection, system and information integrity, and supply chain risk management. This standard facilitated the development of NIST CSF.

NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organisations, is the simplified version of the NIST SP 800-53 standard, originally aimed at governmental subcontractors. This standard can be a good starting point for establishing the most essential controls before expanding the system to include more controls covered by NIST SP 800-53.

The NIST Framework for Improving Critical Infrastructure Cybersecurity, usually referred to as NIST Cybersecurity Framework (NIST CSF) was released in 2013, and its latest revision, version 1.1, was published in 2018. It was originally intended for the critical infrastructure entities, including energy, water, and provision supplies, communications, and healthcare. What singles out these industries is the highest requirements for operation continuity and threat resistance.

NIST CSF is a tool for organizing and improving organisation’s information security strategy. One of the main objectives of the framework is prioritizing cybersecurity layers and supporting investment decisions. It also helps with a general assessment of the maturity of the implemented ISMS.

The framework consists of three components: Core, Tiers, and Profile. The Core component is a list of processes and capabilities comprising organisation’s cybersecurity activities. The Tiers component describes risk management in the organisation with 4 tiers (partial, informed, repeatable, or adaptive) reflecting organisation’s cybersecurity maturity. The Profile component aligns the Core controls with organisation-specific implementation scenarios factoring in business needs.

NIST CSF is a risk analysis-based framework focusing on handling risk by distinguishing five categories of cybersecurity activities and mechanisms corresponding with the phases of risk management: identify, protect, detect, respond, and recover. These categories are described in the Core component. These categories are called functions. The full list of functions is presented in table 1.

Table 1. NIST CSF Structure (adapted from National Institute of Standards and Technology 2014)

Function	ID	Category
Identify	ID.AM	Asset Management
Identify	ID.BE	Business Environment
Identify	ID.GV	Governance
Identify	ID.RA	Risk Assessment
Identify	ID.RM	Risk Management Strategy
Identify	ID.SC	Supply Chain Risk Management
Protect	PR.AC	Identity Management and Access Control
Protect	PR.AT	Awareness and Training
Protect	PR.DS	Data Security
Protect	PR.IP	Information Protection Processes & Procedures
Protect	PR.MA	Maintenance
Protect	PR.PT	Protective Technology
Detect	DE.AE	Anomalies and Events
Detect	DE.CM	Security Continuous Monitoring
Detect	DE.DP	Detection Processes
Respond	RS.RP	Response Planning
Respond	RS.CO	Communications
Respond	RS.AN	Analysis
Respond	RS.MI	Mitigation
Respond	RS.IM	Improvements
Recover	RC.RP	Recovery Planning
Recover	RC.IM	Improvements
Recover	RC.CO	Communications

The **Identify** core function is aimed at managing cybersecurity risk to organisation's resources, including information, equipment, human resources, and IT systems. This function emphasizes the importance of business context and critical resources when analysing relevant risks. The activities that fall under this category include identifying tangible and intangible assets to create an inventory, identifying business environment, identifying applicable legal and regulatory requirements, identifying vulnerabilities and threats, and defining risk management strategy, including cybersecurity capabilities, risk tolerance, and response.

The **Protect** core function defines the safeguards necessary to protect critical processes and information and contain the potential cybersecurity incidents. The activities include implementation of IAM, including physical and remote access; raising security awareness amongst personnel, including admin and other role-based trainings; information protection processes and procedures in accordance with the CIA triad; assets maintenance; and implantation of protective technology layers.

The **Detect** core function implies detecting security incidents, such as anomalous activities and cybersecurity events, that might threaten information security and organisation's critical operations. The activities include continuous security monitoring and active detection processes. The goal is to notice and address security events in a timely manner.

The **Respond** core function includes the follow-up activities for the situations when a security incident was detected, namely planning the response in accordance with the established procedure, communicating the incident to the reporting chain, investigating the incident and its root cause, mitigating the effect of the incident, and improving cybersecurity activities with the goal of preventing similar incidents in the future. The activities are aimed at containing and treating the incident.

The **Recover** core function encompasses all the activities related to business continuity maintenance, such as data backup and replication, restoration of data and services, and resilience of infrastructure. The goal is to ensure timely return to normal operation. (National Institute of Standards and Technology 2014.)

When aligning organisation's cybersecurity activities with the framework, each activity gets a label corresponding with one of these functions. For example, reviews and inventory would fall under the Identify category, running an active AV is a Protect activity, IDS (Intrusion Detection System) and SIEM (Security Information and Event Management) monitoring tools go under the Detect label, incident management procedures are labelled as Response, and data backups are under Recovery.

NIST SP 1800 are a series of guides on the NIST SP 800 standards and framework, providing specifications, configurations, implementation guidance, and real-world examples based on various products. In addition, there is a separate publication, NIST SP 1271, on getting started with the NIST Cybersecurity Framework. (Kirvan & Granneman 2021.)

NIST also has published the Guide for Conducting Risk Assessment (NIST SP 800-30), framework A System Life Cycle Approach for Security and Privacy (NIST SP 800-37),

guidance on Managing Information Security Risk (NIST SP 800-39), Computer Security Incident Handling Guide (NIST SP 800-61), and many other standards that can be used in sector-specific IT environments on all stages of ISMS development, implementation, and operation.

3.2 National Cybersecurity Requirements in Finland

The Security Committee of Finland (Turvallisuuskomitea in Finnish) is a permanent contingency planning body situated at the Ministry of Defence that supports the Government and ministries in matters related to comprehensive security. Comprehensive security is a preparedness cooperation model implying collaboration between the government, business, and citizens addressing the vital societal functions.

The Committee was established in 2013 and its activities are regulated by the Government Decree on the Security Committee (77/2013). The responsibilities of the Committee include collecting information required for the development of society's security and preparing recommendations on comprehensive security proactively and by the government's request. During the monthly meetings, the discussions of necessary proactive measures in the context of the societal changes are taking place. The Committee arranges seminars and public discussions for organisations and the business community. It also coordinates the preparedness measures at the state and municipal level for various security situations, including the ones affecting organisations and the business community, as well as the society in general. (Turvallisuuskomitea Puolustusministeriö s.a.).

In addition to the previously mentioned functions, The Security Committee is responsible for monitoring and coordinating the development and implementation of Finland's Cyber Security Strategy. The strategy is part of the EU Cyber Security Strategy implementation. The latest version was adopted by the Government Resolution on October 3rd, 2019. The strategy outlines national objectives for the development and safeguarding of cyber environment. One of the main goals is facilitating accessibility and reliability of services. Another goal is identification and mitigation of risks and threats endangering vital societal functions. The strategic guidelines include three components:

1. Development of international cooperation: establishing Finland's cyber security integrating international laws and agreements, and with respect for human rights in the cyber space. The guideline emphasises the rule of law, democracy, and transparency. Finland is actively participating in the development of the EU's Common Foreign and Security Policy on Cyber Security, and likewise European strategies and legislation significantly impact national programmes.

2. Coordination of cyber security management: promoting cooperation in planning and monitoring preparedness. For instance, the development of sector-specific programmes requires involvement of the cyber security specialists, cyber research institutes, and key organisations providing public services in the sector. Effective cyber security planning requires dedicated resources and involvement of each administrative branch. To support this guideline, the Cyber Security Director responsible for coordination of the cyber security development on the national level is appointed at the Ministry of Transport and Communication.
3. Development of cyber security competence: the competence on national level is ensured through requirements identification and improving education and research. The goal is to ensure that everyone, including organisations and citizens, is able to operate securely in the digital space. To ensure successful cyber risk management, the authorities and organisations require wide-range expertise from employees and subcontractors. Special attention is paid to the industries that are not providing security-related products and services directly, but are fundamentally affected by the cyber risks, and whose activities are also vital based on the role they play in the functioning of society. These services include telecommunications, production and provisioning of energy resources, financial and healthcare sectors. The defined strategic measures promoting cyber security competence are trainings and programmes for vocational education and universities; high requirements for cyber professionals involved in the nationally critical areas; promotion of national research, development, and testing; improvement of national system for training and exercising cyber security aimed at public administration, business community, and citizens; raising awareness amongst public administration, organisations, and population.

(The Security Committee 2019.)

Along with this general strategy, there is a variety of governmental and non-governmental cybersecurity control frameworks applicable to organisations covering industry-specific and product-specific controls and referred to by the national laws and regulations.

3.2.1 VAHTI

The Ministry of Finance established the Governmental Information and Cyber Security Management Board (VAHTI) as an entity responsible for steering, developing, and coordinating central government information security. Since 2020, the entity is operating as the Digital and Population Data Services Agency. VAHTI coordinates governmental information security policy and guidance matters. The main goal is safeguarding the public administrative activities and ICT services and enabling safe procurement and integration of

new technologies. VAHTI also promotes implementation of national programmes and strategies related to information security, including the national Cyber Security Strategy.

VAHTI has prepared instructions for various actors in the public administration from multiple perspectives to support the government's needs. Some examples of VAHTI instructions are Security Management Guide (VAHTI 2/2011), Information Security Assessment Guide (VAHTI 2/2014), Security Incident Management (VAHTI 8/2017), and Risk Management Guidance (VAHTI 22/2017). There are also documents on a variety of specific topics, such as business continuity management, governmental ICT procurement, secure application development, social media security, encryption policies, and logging.
(Digital and Population Data Services Agency 2020).

3.2.2 Katakri

Katakri (Kansallinen turvallisuusauditointikriteeristö) is a Finnish Information Security Audit Tool for Authorities published by the National Security Authority (NSA) of Finland. It was originally developed by the Ministry of Defence as the national security audit criteria in 2009. The latest, fourth, version was published in 2020, but the 2015 version is still widely used for auditing and referenced by the legislation. The steering group involved in the creation and review of the document involved industry professionals, as well as representatives of the Ministry of Finance, Ministry for Foreign Affairs, Ministry of Transport and Communication, Ministry of the Interior, Ministry of Defence, and the Prime Minister's Office (National Security Authority of Finland 2020).

The tool is freely available and can be used by organisations voluntarily to assess their information security posture. Katakri's requirements are grounded on baseline international security standards and Finland's legislation. The criteria are focused on the security of Classified Information in accordance with the Act on Information Management in Public Administration (906/2019) and the Government Decree on Security Classification of Documents in Central Government (1101/2019).

Katakri is comprised by three major subdivisions: security management, physical security, and information assurance. Each subdivision is marked with a letter and contains enumerated requirements, so the requirements are referred to by the combination of the corresponding subdivision letter and number of the requirement.

1. Security Management (T): the goal is to ensure effective governance of information security through functional procedures and adequate personnel security measures. The subdivision includes 13 requirements covering general security

principles and guidance, tasks and responsibilities of the security management, information security risk management, handling exceptions and malfunctions, security event management, change management, information classification, personnel assessment, confidentiality agreements and NDAs, security training, access rights, and minimal access principle.

2. Physical Security (F): the goal is to secure the physical environment where information is handled. It includes 8 security areas, each comprised by multiple requirements. The requirements cover physical security goals, relevant risk evaluation, choosing physical security measures, defence-in-depth principle, storage and handling of information, protection of security areas, and data security requirements. The security areas are additionally divided into administrative areas and secured areas, including technically secured areas. The selected security measures should be based on the evaluation of physical security measures presented in figure 8, supported by the continuous assessment of related risks and threat analysis.

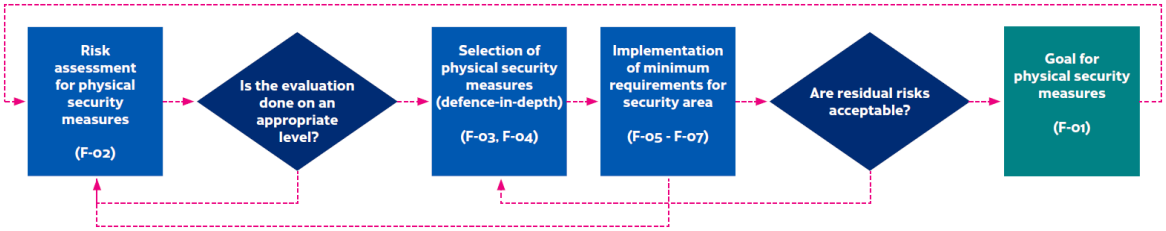

Figure 8. Physical Security Measures Evaluation Process (National Security Authority of Finland 2020, 23)

3. Information Assurance (I): the goal is to secure digital environment by setting requirements for the IT systems and related assets. This is the most technically saturated part, as it provides a lot of configuration requirements for the IT components. With a total of 21 compound interconnected requirements, this part covers such areas as secure connections (including management and admin connections), transfer of classified information between and outside the physically protected areas, cryptography, network architecture, network segmentation and filtering, principle of least privilege and access rights, actor identification, defence-in-depth principle, malware protection, tracing security events, incident detection and recovery, secure information processing environment throughout lifecycle (hardening, system monitoring, attack resilience, software vulnerabilities management, backups, information retention and disposal), change management, and remote access.

Katakri also defines the correspondence of Finnish national classification of information security levels to the international one as follows: Finnish classification level II equals SECRET, level III equals CONFIDENTIAL, and level IV equals RESTRICTED (National Security Authority of Finland 2020).

The requirements set by Katakri can be implemented through a variety of measures making it adaptable for different systems and services. Nonetheless, to facilitate successful implementation the document provides specific examples in the Additional Information field, including the procedures to reach minimal protection level. The implementation examples are based on VAHTI instructions and recommendations of the Information Management Board. The fourth version pays special to the development of secure data processing environments, meaning that the tool can not only be used to assess organisation's security maturity, but also to establish secure development practices. Organisations can be audited against Katakri and obtain respective certification.

3.2.3 PiTuKri

PiTuKri, the Criteria to Assess the Information Security of Cloud Services, is developed and published by the Finnish Transport and Communications Agency (Traficom) and National Cyber Security Centre for the Finnish authorities with the goal of improving the security of information processed in cloud computing environments. It was originally published in 2019, and the updated 1.1 version was published in March 2020. It is developed taking into account the national legislation, the international standards (including ISO/IEC 27001), and Katakri criteria.

Intended as a tool for assessing security of cloud systems for governmental needs, it is aimed at information of protection level IV according to the national classification (RESTRICTED according to the international classification). It can also be used by the cloud service providers to establish and assess security of operations. The requirements have to be considered in the context of the shared responsibility model, depending on the capacity of the provided services. NIST (NIST SP 800-145 The NIST Definition of Cloud Computing 2011, 2-3) defines the cloud computing service models as follows:

- Infrastructure as a Service (IaaS): consumer is provided the capability to provision fundamental computing resources (e.g., processing, storage, networks) for deploying and running arbitrary software, including OS and applications.
- Platform as a Service (PaaS): consumer is provided the capability to deploy consumer-created or procured applications using tools (e.g., programming languages, libraries, services) supported by the provider onto the cloud infrastructure.
- Software as a Service (SaaS): consumer is provided the capability of using the provider's applications running on a cloud infrastructure.

Standard shared responsibility model is presented in table 2.

Table 2. Shared Responsibility Model (adapted from Traficom 2020, 10)

IaaS	PaaS	SaaS	
Interface	Interface	Interface	
Application	Application	Application	Customer
Solution Stack	Solution Stack	Solution Stack	
Operating System	Operating System	Operating System	
Virtualization	Virtualization	Virtualization	
Compute & Storage	Compute & Storage	Compute & Storage	Provider
Networking	Networking	Networking	
Facility	Facility	Facility	

Based on PiTuKri's definition, the cloud services platform is the responsibility of the provider, while customer's system in the cloud, processing environment, and remote access environment are the responsibility of the customer (depicted in figure 9). Taking this into account, specific PiTuKri requirements can be applied only to the service provider's domain, only to the customer's domain, or to both. It is also usually justified to include all the involved third parties. For example, if a customer uses PaaS service model and has custom application add-ons created by an independent developer, it makes sense to evaluate the security of the software development practices followed by the developer.

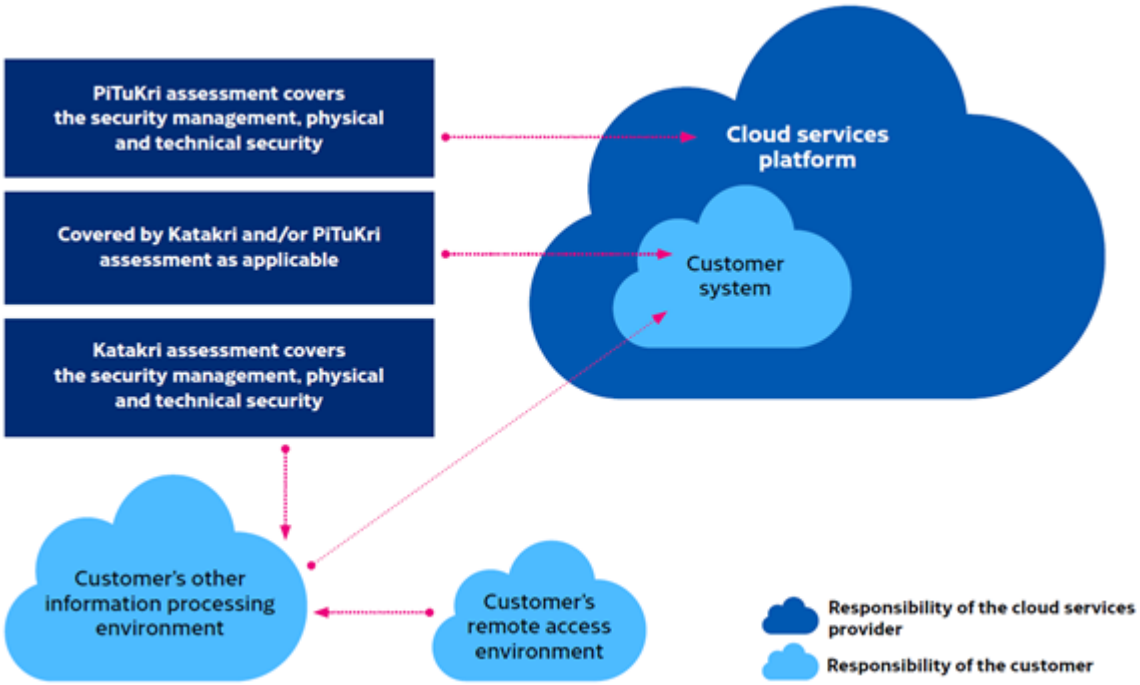

Figure 9. PiTuKri Division of Responsibility for Processing Environments (Traficom 2020, 4)

The document is divided into 11 subdivisions. The first subdivision, framework conditions, can be used to direct further assessment in accordance with the following subdivisions. It defines the requirements related to system description and legislation-derived risks, as well as outlines possibilities for assessment based on the type of information handled by the service. Other relevant factors include physical location of the information throughout its lifecycle and local laws applied, physical location of the functions (such as system maintenance and administration, backups, data replication), other parties involved (subcontractors, outsourcing), SLAs (Service Level Agreements) and contracts, applicability sector (public or private). The framework conditions only address general risks and complying with its requirements does not provide information protection without fulfilling the applicable requirements from the following subdivisions, 2 to 11, that cover security management, personnel security, physical security, communications, IAM, information system security, encryption, operations security, transferability and compatibility, change management, and secure system development.

PiTuKri is a flexible guidance that has been designed to accommodate a variety of cloud services with different use cases. It promotes taking into consideration the results of internal and external evaluation of the environment, basing security requirements on continuous risk assessment, and interpreting requirements for adequate implementations on a case-by-case basis, keeping in mind the purpose and needs of each system.

3.2.4 Protecting Personal Data of Finnish Citizens

Protection of personally identifiable information (PII) if one of the key areas of information security. NIST (NIST SP 800-79-2 2015, 46) defines PII as any form of information that allows to reasonably assume the identity of the individual to whom the information is related by direct or indirect means. In Finland, the government facilitates protection of PII on the legislation level, as well as by supporting relevant research, and establishing responsible authorities to develop recommendations, guidelines, requirements, and regulations.

One of the major categories of PII is healthcare data, both named and anonymized, whether it is stored in plain text or encrypted. Kanta Services is a national, legislation-based archiving service functioning under the Act on the Electronic Processing of Client Data in Healthcare and Social Welfare (784/2021). The Act came into effect on November 1st, 2021, and it requires all entities in the healthcare and social welfare sector providing public services to enter patient data in the national archive. For instance, information regarding COVID-19 vaccination was stored in the Kanta Services, and citizens had to access their personal profile on the Kanta.fi website in order to receive their vaccination certificates. The deployment of the services is also mandatory for the private sector, as long

as the organisation uses an information system for processing their patients' data. The main goal is to ensure secure and reliable processing of the citizens' PII. (Kanta 2021.)

Through Kanta Services, citizens can access their medical records, prescriptions, medical certificates, and reports, as well as order repeat prescriptions when necessary. Kanta also maintains a pharmaceutical database with information on medications, prices, and availability. For the healthcare and social welfare services, the system acts as a centralised electronic archive of patient data. Doctors and dentists can issue online prescriptions through the service. In general, Kanta promotes continuity of healthcare and welfare services and patients' safety. The key data protection principles followed by Kanta include preventing unauthorized access, performing continuous monitoring of data processes, and ensuring availability, secure storage, and protection of the entered data.

Even when PII is anonymized and used for research, education, statistics, and authority reporting purposes, it still has to be protected under the European (GDPR) and Finnish legislation. The Act on the Secondary Use of Health and Social Data (552/2019) sets requirements for the secure processing environments where permit holders can access and handle data for the purposes other than the purpose for which the data was originally collected. The permits are issued by Findata, the Social and Health Data Permit Authority. In most cases, users are granted remote access to Findata's secure environment. However, for the cases where data is to be transferred to the permit holder for processing, the permit holder is responsible for demonstrating that the data will be processed in a controlled environment compliant with the legal data protection requirements. The environment is required to provide the same security and protection level as Findata's own operating environment.

Findata publishes the regulation on the Requirements for other service providers' secure operating environments (Findata 2022a). The latest version of the regulation became effective in January 2022. Annex 1 of the regulation specifies the requirements which can be used as a control framework for evaluating security of the processing environment. The requirements cover two major areas: technical specifications of the environment (IAM, protecting the environment, logging, system management and monitoring, data disposal) and reliability of the operator (data protection responsibilities, premises security, personnel) (Findata 2022b). The information systems are required to keep a record log reflecting full processing history: who, how, and when processed the data.

Compliance with the Acts and implementation of the requirements in the information systems intended for processing PII is administered by Valvira, the National Supervisory Au-

thority for Welfare and Health. The systems must fulfil the requirements on interoperability, information security, and functionality before deployment. The system supplier is responsible for demonstrating compliance by notifying Valvira of the new data system and completing the system form including adequate technical evaluation. The supplier is also compelled to keep the system updated, actively monitor its operation, analyse the results, and report any significant deviations that might pose a risk to the safety of data. All the systems are categorized by class: Class A for the Kanta Services and systems connected to Kanta directly or through an intermediary service, as well as the intermediary service itself, and Class B for the other data systems. Valvira maintains and publishes the register of all the deployed data systems on the official website. (Valvira 2022.)

3.3 Compliance with Cybersecurity Standards and Legislation

This chapter gave an overview of a variety of international and national cybersecurity standards and regulations based on the legislation and industry best practices. Organisations must comply with the requirements dictated by the laws and regulations and. On top of that, they can choose to comply with voluntary standards based on the sector of operation or specifics of the deployed technologies to ensure business continuity and strengthen their position on the market.

In some cases, an organisation will need to comply with multiple requirements frameworks. For example, if the organisation operates on the international level and processes personal data of citizens from multiple states, they will need to look into legislation of each state for the personal data processing requirements. Even if the organisation operates only within one country, meaning their organisational and business data never leaves the country and all their system development, maintenance, and administration is performed on the territory of that country, they might want to comply with the international standards to improve their security posture and work with the customers worldwide.

Chapter 4 will explore the means, methods, and points to consider when aligning ISMS with multiple cybersecurity control frameworks based on the example of the international ISO/IEC 27001 information security standard and Finland’s national Katakri criteria for information security assessment.

4 Establishing Organisation's Information Security Management in Compliance with Finland's National Requirements

As demonstrated by the standards, regulations, and frameworks reviewed in the previous chapter, there are different approaches and recommendations regarding information security management. These recommendations can be used to establish baseline security in the organisation.

Organisations might choose to achieve multiple certifications for business continuity, legislative, regulatory, financial, and reputational reasons. ISO/IEC 27001 standard notes that additional security controls and measures might be required for enhanced security. However, it is important to mention that a large number of implemented requirements and followed security standards does not automatically result in a better system and information protection for the organisation. In general, an organisation can establish the benchmark for its security posture based on either of the security control frameworks, as long as all the relevant security measures are in place.

When pursuing compliance with multiple control frameworks, it is essential to see which requirements are shared, and which need to be considered and implemented separately. This chapter details the process of aligning two control frameworks based on the example of ISO/IEC 27000 ISMS standards (mainly, ISO/IEC 27002:2022, Information security controls, with some references to ISO/IEC 27001:2013, Information security management systems requirements) and Katakri Security Audit Tool. It makes the most sense to choose the updated version of the ISO/IEC 27002 standard for this analysis due to its functional and structural similarities to Katakri, highlighting the substantial contextual differences between the two frameworks.

It is significant to note that the terminology might vary between the two frameworks. In this research, the analysis was performed on conceptual level, taking into account the implications of the requirements rather than the strict wording. This can be justified by the fact that controls are often up for specialists' interpretation, as most specifications are presented in the form of recommendation, with the level of protection the control implementation provides being the decisive factor.

4.1 Baseline Security

As mentioned in the introduction to this chapter, the baseline security level in the organisation can be achieved by complying with the applicable security requirements from either of the frameworks. The requirements outlined by Katakri were originally developed based

on the best practices provided in the ISO/IEC 27000 standards. The difference is that they have been adapted to accommodate the needs of the national authorities of Finland.

This is consistent with the ISO/IEC 27001 Clause 4.2 (2013) which states that “the organisation shall determine interested parties relevant to ISMS and the requirements of these interested parties relevant to information security”. The interested parties in this case are also the government and regulatory authorities, and the requirements include legal and regulatory requirements imposed and enforced by these interested parties.

ISO/IEC 27002 classifies all the controls into 4 big categories: people, physical, technological, and organisational. Katakri splits the criteria into 3 subdivisions: security management (administrative information security measures and personnel security), physical security (general requirements, security area requirements, and data security requirements), and information assurance (communications, system, and operations security).

Table 3. Katakri 2020 and ISO 27002:2022 Correspondence Table

Katakri 2020		ISO 27002:2022	
Subdivision	**Name**	**Clause**	**Requirements**
T: Security Management	Administrative information security measures	5 Organisational Controls	5.1 – 5.37
	Personnel security	6 People Controls	6.1 – 6.8
F: Physical Security	General requirements	7 Physical Controls	7.1 – 7.14
	Requirements for Security Areas		
	Data security requirements	5 Organisational Controls + 8 Technological Controls	5.14, 5.33, 5.37, 8.10, 8.12, 8.15
I: Information Assurance	Communications Security	8 Technological controls	8.11, 8.12, 8.20 – 8.23
	System Security		8.2 – 8.5, 8.7, 8.15 – 8.18, 8.24, 8.26, 8.29
	Operations Security		8.1, 8.8 – 8.10, 8.13, 8.19, 8.28, 8.31 – 8.34

As can be seen from the table 3, ISO/IEC 27000 standards and Katakri criteria cover a lot of common areas. Katakri also contains multiple references to ISO/IEC 27000 series in the additional information sources section. Katakri’s section Administrative information security measures in the Subdivision T: Security Management has strong correspondence to the ISO/IEC 27002’s Clause 5 (Organisational controls). Personnel Security section of Katakri’s Subdivision T can be linked to Clause 6 (People controls). Subdivision F: Physical Security is similar to Clause 7 (Physical controls). However, Katakri also includes Data security requirements in the Physical Security subdivision covering information stored in the non-digital format. This is not specifically addressed by ISO/IEC 27002, as most of the procedures encompass organisation’s information in all forms, so these issues are mostly

covered in Clause 8 (Technological controls). Subdivision I: Information Assurance is closely connected to Clause 8 (Technological controls), but also has a few links to Clause 7 (Physical controls).

In general, both frameworks promote the overarching principle of defence-in-depth and security by design, meaning that security measures are integrated with all the operations, and each function is protected by multiple organisational, physical, and technological security layers.

Another baseline security principle is related to access rights. Access rights are to be granted based on the principles of least privilege, need-to-know, and segregation of duties, meaning that the user only gets access to the assets, functions, and information that are necessary to perform their immediate duties and the access is ceased as soon as it is no longer authorized or required.

The full list of the ISO/IEC 27002:2022 controls and the Katakri 2020 criteria are attached in Appendices 3 and 4 respectively. The next section explores the results of a more detailed comparative analysis of the two frameworks. (National Security Authority of Finland 2020, ISO/IEC 2022.)

4.2 Comparative Analysis of ISO/IEC 27001 and ISO/IEC 27002 vs. Katakri 2020

Even though both frameworks cover similar areas and address a lot of the same issues and security principles, there are some major differences in focus, scope, and individual requirements.

First of all, there are differences in the general structure. ISO/IEC 27001 Annex A lists controls to be implemented and ISO/IEC 27002 provides implementation guidance. Each Katakri criterion has the Additional Information section, where specifications are provided. This section often contains examples of implementation with a reference to the information protection level to which the particular example applies.

Unlike ISO/IEC 27001, when Katakri defines the requirements and provides implementation examples, it characterizes them as applicable for a certain classified information protection level (PL). PL IV corresponds with RESTRICTED security level international classification, PL III corresponds with CONFIDENTIAL, and PL II is SECRET. Katakri does not address PL I (TOP SECRET) requirements. Unclassified national information that is not considered public is to be treated as equal to PL IV.

On the per-requirement structural level, each control in ISO/IEC 27002 includes control description, control objective (purpose), implementation guidance, and additional information sections. An example of ISO/IEC 27002 control can be seen in figure 10. In the new 2022 version tagging was introduced, labelling each control by type, information security properties, cybersecurity concepts, operational capabilities, and security domains. The control types include preventive, detective, and corrective tags.

5.29 Information security during disruption

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond	#Continuity	#Protection #Resilience

Control

The organization should plan how to maintain information security at an appropriate level during disruption.

Purpose

To protect information and other associated assets during disruption.

Guidance

The organization should determine its requirements for adapting information security controls during disruption. Information security requirements should be included in the business continuity management processes.

Plans should be developed, implemented, tested, reviewed and evaluated to maintain or restore the security of information of critical business processes following interruption or failure. Security of information should be restored at the required level and in the required time frames.

The organization should implement and maintain:

a) information security controls, supporting systems and tools within business continuity and ICT continuity plans;

b) processes to maintain existing information security controls during disruption;

c) compensating controls for information security controls that cannot be maintained during disruption.

Other information

In the context of business continuity and ICT continuity planning, it can be necessary to adapt the information security requirements depending on the type of disruption, compared to normal operational conditions. As part of the business impact analysis and risk assessment performed within business continuity management, the consequences of loss of confidentiality and integrity of information should be considered and prioritized in addition to the need for maintaining availability.

Information on business continuity management systems can be found in ISO 22301 and ISO 22313. Further guidance on business impact analysis (BIA) can be found in ISO/TS 22317.

Figure 10. Example of a Control Structure (ISO/IEC 27002:2022, 48)

Katakri defines a criterion description and clarifies it in the Additional Information field. The Additional Information field contains general explanations and specifications of the control, as well as implementation examples for different classified information protection levels. Katakri also provides references to the relevant information sources, such as legislation and security standards. An example of a Katakri criterion is presented in figure 11.

I-10 DEFENCE IN DEPTH – TRACEABILITY OF SECURITY EVENTS

Requirement	§ Source (906/2019 and/or 1101/2019)	§ Source (2013/488/EU)
1. **In order to detect unauthorised changes or other unauthorised or inappropriate information handling within the information-processing environment, reliable methods have been taken into use for tracing the security events.** 2. **The use of information systems and disclosure of their information will be logged in case the use of the information system requires identification or other methods of signing in. The idea to collect log information is to follow the use and disclosure of the information and to find out reasons for technical system failures.** 3. **The use of Classified Information belonging to national classification levels II and III has to be registered into an electronic log, information system, case register of as a part of information itself (e.g. part of a document).**	1. 906/2019 sections 17, 15, 1101/2019 section 7 2. 906/2019 section 17 3. 1101/2019 section 14	1. Annex IV (16), annex III (18 and 21) 2. – 3. –

Additional Information

In general: Traceability refers to recording the events of the system environment so that, in abnormal situations, it is possible to find out what measures had been taken in the environment and by whom, and what effects such measures have had. Essential recordings typically include the log data of fundamental network devices and servers. In addition, log data of workstations, etc. are also very often covered by this.
The coverage requirement can, in most cases, be met by checking that logging is on at least for workstations, servers, network devices (especially firewalls, but also for software firewalls on workstations). It should be possible to afterwards check from the network device logs as to what management functions were performed on the network device, when and by who. Event logs should be compiled of the use of the system, user activities as well as security-related functions and exceptions.

A recommended method to protect the logs is to forward all essential logging information to a strongly safeguarded logging server (or servers), the information content of which is regularly backed up. The logging server(s) must be at environment belonging at least to the same classification level as the log source environment.

Collection and recording of log data needs to be done in a way where the removal of changing of log data can be detected even in situations, where e.g. the log source and the log collector are disconnected. Correspondingly, the collection of log data and their backups from workstations permanently disconnected from the network requires a regular process in place. To support the legal protection of administrators and promote investigation of suspected security breaches, it is recommended to separate tasks so that the logging data maintenance duty is separated from other maintenance duties. In the implementation of traceability also situations, when the individual who has logged in to the system has the possibility to function by using another user account (user impersonation) has to be taken into account. The functioning of logging data storage and analysis software must also be monitored and possible failures have to be detected in a short time frame (e.g. within 24 hours after the log source has stopped to deliver the logs).

I-10 DEFENCE IN DEPTH – TRACEABILITY OF SECURITY EVENTS

The log data storage periods must take into account the needs of the use case in question. For example, for information processing and delivery logs it may be advisable to require storage durations which differ from the storage duration for logs, which are collected to sort out exceptional situations In the activities of the authorities, for example, statutes of limitation in the criminal justice can typically lead to a required storage period of at least five years. As a general practice log data for 6 months is available on a real-time basis and earlier log data will be available within a couple of days, when needed. Different cases for handling log data are covered also in the recommendation of the Information Management Board (2020:21, chapter 7).

In the implementation it should be taken into account that the duration and storage capacity of the logs will be sufficient (normally needs to be increased). Recommendation: to reserve enough capacity, the estimation can be based on the processing environment. Definition of an adequate duration can be done by e.g. calculating the storage capacity sufficient for one month and using this information to determine the storage capacity needed for the storage duration. Note: it is advisable to reserve some buffer capacity, as situations change and because certain type of attacks increase log activities a lot.

Example of implementation: on processing environments belonging to classification level IV (RESTRICTED), the requirement can be fulfilled by putting into force the following:
1. A policy document defining the generation, release, alarm and follow up of the logs has been taken into actual use. This policy has been written taking into account the particular operational requirements.
2. Logs make it possible to detect the security breaches or attempts to such afterwards.
3. Essential recordings are kept for at least six months, unless laws and regulations or separate contracts specify a longer retention period. Processing logs and recordings following the requirements set for, e.g., periods of limitation of the information in criminal justice cases are stored for at least five years.
4. Log files and respective register services are protected against unauthorised access (user rights management, logical access control).) A policy document defining the generation, release, alarm and follow up of the logs have been taken into the actual use. This policy has been written taking into account the particular operational requirements.

On classification levels III and II this requirement may be fulfilled by using the following procedures in addition to the points 1-4 above:
5. Essential recordings are kept at least for five years, unless laws and regulations or separate contracts specify a longer retention period. Recordings with very little value to, e.g., sorting out exceptional situations or to periods of limitation of the information in criminal justice, may be retained a shorter period, for example 2-5 years.
6. Log files are backed up regularly.
7. Clocks of all relevant information processing systems within security domain must be synchronized to a single reference time source.
8. Procedure covering the integrity of the logs has been taken into use.
9. Handling and usage of log files is registered.

Other sources of information: CIS Critical Security Controls (v7.1) / 6; BSI IT-Grundschutz-Compendium Edition 2019; The United States Government Configuration Baseline (US- GCB); SFS-EN ISO/IEC 27002:2017 12.4.1, 12.4.2, 12.4.3, 12.4.4, 18.1.3; VAHTI 3/2009; Recommendation of the Information Management Board (2020:21, chapter 7); PiTuKri JT-01

Figure 11. Example of a Criterion Structure (National Security Authority of Finland 2020, 85-86)

One of the main distinctions is that ISO/IEC 27001 promotes risk-based approach, meaning that the control framework can be modulated to fit organisation's needs based on the results of risk analysis through an SoA. Organisations are encouraged to evaluate how ef-

fective the implemented security controls are and how efficient the investment into the security measures would be based on the identified risks. Katakri, while highlighting the importance of risk assessment, sets a binding list of criteria, where each requirement on the applicable information classification protection level is mandatory to comply with. The risk assessment instructions can be found in the criteria T-03 (Management of information security risks), F-02 (Risk assessment of physical security measures), F-03 (Selection of physical security measures), and I-09 (Protection against malware). Risk assessment modulates the level of security that is required. Therefore, some Katakri requirements might not be as relevant for an organisation, but still must be implemented. The area where Katakri allows some flexibility is implementation measures, as long as the chosen measures provide an equal level of protection to the required one. (National Security Authority of Finland 2020, ISO/IEC 2022.)

To provide a structured detailed analysis of the individual requirements, this research has categorized the requirements from both frameworks into 4 sub-sections. The areas of Katakri 2020 and ISO/IEC 27002:2022 addressed in each of the following sub-sections is presented in table 4.

Table 4. Specification of Sub-sections and Corresponding Katakri 2020 and ISO/IEC 27002:2022 Requirements

Sub-section	Katakri	ISO/IEC 27002
4.2.1 Governance Requirements	• T: Security Management (Administrative information security measures)	• 5 Organisational Controls
4.2.2 HR Requirements	• T: Security Management (Personnel security)	• 6 People Controls
4.2.3 Physical Security Requirements	• F: Physical Security (General requirements) • F: Physical Security (Requirements for Security Areas)	• 7 Physical Controls
4.2.4 Technical Requirements	• F: Physical Security (Data security requirements) • I: Information Assurance (Communications Security) • I: Information Assurance (System Security) • I: Information Assurance (Operations Security)	• 5 Organisational Controls • 8 Technological controls

4.2.1 Governance Requirements

Security governance addresses administrative procedures, company policies, operation guidance, segregation of duties, classification of assets (including information), compliance, and other managerial issues.

Management responsibilities are outlined by both frameworks, with T-01 criterion in Katakri and control 5.4 in ISO/IEC 27002. Senior management is expected to introduce and support security principles, policies, and procedures, as well as monitor organisation's adherence to them on a high level. Segregation of duties is also addressed by the frameworks. Criteria T-02 in Katakri and controls 5.2 and 5.3 in ISO/IEC 27002 require defined tasks and structure, in particular for the roles involving managerial or information security-related duties.

In addition, ISO/IEC 27002 controls 5.5 and 5.6 declare that an organisation should establish and maintain contact with relevant authorities and special interest groups. This requirement is not explicitly mandated by Katakri. However, Katakri T-07 on management of security events states that relevant security events must be immediately reported to the competent authorities. Management of security events is split into 4 controls in ISO/IEC 27002: 5.24 on incident management planning and preparation, 5.25 on assessment and decisions on information security events, 5.26 on response procedures, 5.27 on lessons learnt, and 5.28 on collection of evidence. Related ISO/IEC 27002 control 5.29 (Information security during disruption) and the corresponding Katakri criterion T-06 (Malfunctions and exceptional situations) declare that organisations should plan for maintaining appropriate level of information security during exceptional situations and minimize the effects of disruptions in the system operation and malfunctions.

Katakri pointedly addresses risk management in criterion T-03. This is an underlying concept in the whole ISO/IEC 27000 series and is addressed in the new clause 5.7 Threat intelligence added in the 2022 version of the ISO/IEC 27002 standard. On top of that, it is specified in the introduction that security controls implementation should be based on the results of risk analysis, and risk management is pointed out as one of the main responsibilities of the management and people in the security-related roles.

Katakri T-04 Security guidance requirements correspond with the ISO/IEC 27002 controls 5.1 (Policies for information security), 5.8 (Information security in project management), 5.10 (Acceptable use of information and other associated assets), 5.31 (Legal, statutory, regulatory, and contractual requirements), and 5.37 (Documented operating procedures).

Katakri has broader approach, while ISO/IEC 27002 is more detailed, but these requirements essentially address the availability of the necessary documentation on information security in the organisation, including policies and instructions.

Additionally, ISO/IEC control 5.35 states that independent review of the approach to managing information security, including all the components, should be performed at regular intervals and after significant changes. There is no specific requirement for this in Katakri.

Katakri T-08 corresponds to ISO/IEC 27002 control 5.12 (Classification of information). It also has links to controls 5.9 (Inventory of information and other associated assets) and 5.13 (Labelling of information). Katakri T-08 has a unique requirement that applies only to the authorities: the authority should have instructions for information classification and label information by protection level. As discussed previously, this is necessary to identify the level of security measures to be adopted by the organisation or by the units that handle information of a specific protection level.

ISO/IEC 27002 has several controls on the supplier management: 5.19 (Information security in supplier relationships), 5.20 (Addressing information security within supplier agreements), 5.21 (Managing information security in the ICT supply chain), and 5.22 (Monitoring, review and change management of supplier services). Katakri lacks corresponding instructions, it is only implied that all suppliers should have sufficient levels of security implemented, exercise secure software development practices, and supplier's bulletins and recommendations should be followed by the adopting organisation. This is specified in Katakri I-19, Security throughout the information processing environment lifecycle - Management of software vulnerabilities.

ISO/IEC 27002 also includes controls 5.32 (Intellectual property rights), 5.33 (Protection of records), and 5.34 (Privacy and protection of PII). This is not pointedly addressed by Katakri, but classified information protection is the overarching principle of the tool. On top of that, there are dedicated laws on protection of PII effective on the national (addressed in section 3.2.4 of this research) and international level, the main one being GDPR (addressed in section 3.1.3 of this research).

In the new 2022 version of ISO/IEC 27002, clause 5.23 was added, covering information security of cloud services. Katakri does not address this issue in either of the criteria. Instead, in the introduction to Subdivision I: Information Assurance, it mentions that reliance on the cloud-based technologies does not bring any fundamental changes to the basic risks, and references PiTuKri as the source of information on cloud-specific risks and related minimal controls. (National Security Authority of Finland 2020, ISO/IEC 2022.)

4.2.2 Human Resources Requirements

Personnel plays a major role in the organisation's information security. It is important to raise security awareness because an oversight of a single employee can lead to a large-scale breach. HR operations (start of the employment, change of position, ending the employment) should also incorporate security practices, especially due to their direct connection to the level and scope of access a person gets to the system and its information.

On the general level, Katakri T-05 states that there should be sufficient information security expertise in the organisation. This is also implied by ISO/IEC 27002 controls 5.1 and 6.3.

Both Katakri (criterion T-12) and ISO/IEC 27002 (control 6.3) lay out the need for security trainings and raising awareness amongst employees. Recommendations include conducting regular trainings on the role-specific activities, company policies, updates, applicable legislation, and contractual requirements. Katakri specifically points out the need for trainings on handling Classified Information. Organisation should assess and monitor knowledge levels at the end of the training, and the training materials, records, lists of participants, and resulting company-wide statistics are to be documented.

Changes in access to assets (including systems and information) throughout the employment are addressed by Katakri T-09 (Changes in the handling of classified information throughout the employment), ISO/IEC 27002 control 6.2 (Terms and conditions of employment), and ISO/IEC 6.5 (Responsibilities after termination or change of employment). Related NDAs and confidentiality agreements are covered by Katakri T-11 and ISO/IEC 27002 control 6.6.

Both frameworks point out the need for assessment of trustworthiness and reliability of the employees, which is covered by Katakri T-10 and ISO/IEC 27002 control 6.1. ISO/IEC 27002 also has a dedicated control 6.4 on the disciplinary process, entirely missing from Katakri. (National Security Authority of Finland 2020, ISO/IEC 2022.)

4.2.3 Physical Security Requirements

Physical security covers the security of premises, people working on-premises, and tangible assets, such as equipment and devices. This is an area that is exhaustively covered by Katakri, but only broadly addressed by ISO/IEC 27002. This is justified by the fact that Katakri focuses on facilities where storage and processing of highly sensitive data is performed, therefore requiring special attention to resilience and continuity of physical assets.

Katakri starts with explaining the general goal of physical security, instruction on analysing risks related to physical security, and selection of appropriate physical security measures (Katakri F-01 – F-03). The tool also has technical specifications for physical security measures, such as locks and structures, with links to specific standards (e.g., national technical standards SFS-7020 and SFS-5970 for locks in the secured areas).

Katakri also gives dedicated instructions on information storage and handling within and outside the security areas (Katakri F-04, F-05.8, F-06.10). This is briefly addressed by ISO/IEC 27002 control 7.6 (Working in secure areas).

Protection of physical perimeter is addressed by Katakri F-05.1 and F-06.1, as well as ISO/IEC 27002 controls 7.1 and 7.2. The perimeters and facilities should be equipped with intrusion detection systems as per Katakri F-05.5 and F-06.7, unless 24/7 monitoring or inspection at irregular intervals outside working hours is performed. For ISO/IEC 27002 physical security monitoring is a new requirement added in the 2022 version. Control 7.4 states that continuous monitoring of premises for unauthorized access should be performed.

Management of access rights and visitor access are covered by Katakri F-05.2, F-05.3, and F-06.2 – F-06.4. ISO/IEC 27002 approaches this from the governance perspective, specifying relevant instructions in controls 5.15 – 5.18 on identity management, access control, and access rights. These controls apply to both physical and logical access.

Katakri also pays special attention to preventing different types of espionage through soundproofing and protection from unauthorized observation (Katakri F-05.4, F-05.6, F-06.6, and F-06.8). This is not an area of focus for the ISO/IEC 27002 standard, with only clear desk and screen policy addressed in clause 7.7 stating that sensitive and critical information should not be left on display unattended or unlocked.

Katakri F-05.7 and F-06.9 are unique requirements only applicable to the areas and systems collecting and processing information classified as PL IV (national scale) or SECRET (EU scale). These areas and systems should be regularly inspected technically and physically if the threat of disclosure is evaluated as high or unauthorized access is suspected. There are also requirements for the technically secured areas (Katakri F-07) based on the security regulation of the Council of EU and NATO for the areas where international Classified Information is stored and handled.

ISO/IEC 27002 has some additional requirements for secure and protected equipment siting (control 7.8), protection from power failure and other disruptions connected with the failure of supporting utilities (control 7.11), protection of cables carrying power and data against interceptions, interference, and damage (control 7.12). In addition, there are requirements for equipment maintenance to support CIA of information (control 7.13) and secure equipment disposal (control 7.14), which states that the equipment must be sanitized from any sensitive data and licensed software before disposal or re-use.

ISO/IEC 27002 also has a dedicated clause 7.5 on protection against physical and environmental threats. This is not addressed separately by Katakri, as these issues are already covered by the very detailed specifications for the structures of the facilities. (National Security Authority of Finland 2020, ISO/IEC 2022.)

4.2.4 Technical Requirements

Technical requirements include the controls applicable on all layers of defensive technology implemented in the organisation, covering the areas of access rights management, change management, secure remote operations, network segmentation, communications security, system hardening, activity monitoring, incident detection and response, secure data storage, transfer, and disposal. These requirements are meant to protect the system and its information from internal and external threats, such as human error and cyber-attacks. This component of the general security framework ultimately supports other parts, facilitating business operations and incorporating security measures.

Starting with the network architecture and communications security, both frameworks share similar requirements for network segmentation (Katakri I-01, I-02, and ISO/IEC 27002 8.20, 8.21, 8.22), traffic filtering, and monitoring (Katakri I-03 and ISO/IEC 27002 8.23). Additionally, Katakri outlines the requirements for isolation of the management connections in criterion I-04. ISO/IEC 27002 also has two clauses newly added in the 2022 version: clause 8.11 requires that data is masked in accordance with organisation’s policies and legislation, while clause 8.12 focuses on data leakage prevention measures for systems, networks, and devices storing and processing sensitive information.

Encryption of data at rest and in transit is required to protect data against loss of integrity and unauthorized access. Encryption is covered by Katakri I-05 (Wireless transmission), I-12 (Crypto solutions), I-15 (Electronic transfer of the information), ISO/IEC 27002 control 8.1 (User endpoint devices), and control 8.24 (Use of cryptography).

Compared to ISO/IEC 27000 standards, Katakri has more detailed and comprehensive requirements on handling highly sensitive data. Katakri, for instance, contains requirements for PL II, which are only applicable for organisations dealing with the national information labelled with high secrecy level. Such requirements might not be feasible to implement for organisations that do not deal with governmental work and handling critical information but are mandatory for organisations collecting and processing information classified as PL II on the national scale.

System hardening, and specifically protection against malware and cyber-attacks, are addressed by Katakri I-08, I09, I-13, and ISO/IEC 27002 control 8.7. Change and configuration management, covered by Katakri I-16, are addressed in Clauses 8.32 and 8.9 respectively. Clause 8.9 is a new clause added in the 2022 version of ISO/IEC 27002. Two other controls closely connected to the change and configuration management are control 8.18 on privileged utility programs usage and control 8.19 on software installations on OSs. Vulnerability management is addressed by Katakri I-19 and ISO/IEC 27002 control 8.8. Protection against electromagnetic emanations and electronic intelligence are the focus of criterion I-14 in Katakri. These issues are briefly mentioned in the Physical controls of ISO/IEC 27002, specifically in controls 7.3 (Securing offices, rooms and facilities) and 7.12 (Cabling security).

Both frameworks point out the need for monitoring and logging of the activities, as well as collecting evidence regarding security incidents. These requirements are addressed by criteria I-10 and I-11 of Katakri and controls 8.15 and 8.16 in ISO/IEC 27002. Katakri I-10 also mentions clock synchronisation to support proper functioning of the systems, which is a separate requirement stated in ISO/IEC 27002 control 8.17.

Identification and access rights management are vastly covered by both frameworks, including Katakri criteria I-06 and I-07, and ISO/IEC 27002 controls 8.2 – 8.5. Special attention in this area is paid to remote working and connections. The requirement for establishing secure remote connections is specifically outlined by Katakri I-18 and ISO/IEC 27002 control 6.7.

Secure data retention and disposal is another baseline security requirement. Data backup is addressed in Katakri I-20 and ISO/IEC 27002 control 8.13, and data disposal – by Katakri I-21 and ISO/IEC control 8.10.

One area that is not pointedly addressed by Katakri is secure system development, and the adjacent areas of testing and testing environments. Therefore, if the organisation’s

core activities are connected with software development services, they would have to implement additional controls for this area, other than the ones laid out by Katakri, to ensure comprehensive information security coverage. For example, NIST SP 800-218 Secure Software Development Framework (NIST 2022) focuses on this area. ISO/IEC 27002 also has extensive coverage of this area, including controls 8.25 (Secure development life cycle), 8.26 (Application security requirements), 8.27 (Secure system architecture and engineering principles), 8.28 (Secure coding). Outsourced development, covered by control 8.30, is briefly addressed in Katakri I-13, with the requirement that all acquired systems must be compliant with the legislation.

ISO/IEC 27002 also pays special attention to separation of development, testing, and production environments, as well as secure testing procedures. These issues are addressed by controls 8.29 (Security testing in development and acceptance), 8.31 (Separation of development, test and production environments), 8.33 (Test information), and 8.34 (Protection of information systems during audit testing). Katakri only shortly addresses this in criterion I-19, stating that the testing is to be done in an isolated environment by a small group of users.

Capacity management and redundancy of information processing facilities to ensure availability of data and services, are covered by controls 8.6 and 8.14 respectively in ISO/IEC 27002 but are completely overlooked by Katakri. These requirements support the CIA of data and services by monitoring and adjusting the capacity of the utilized resources to fit the current needs using additional facilities and processing resources. (National Security Authority of Finland 2020, ISO/IEC 2022.)

4.3 Strategic Approach to ISMS Enhancement

After the analysis of the differences and similarities between the two security requirements frameworks, this section is dedicated to some practical guidelines on how to enhance an existing ISMS by adding additional controls with the goal of reaching compliance with multiple standards or regulations. The proposed approach is quite similar to the standard ISMS development process, augmented by incorporating considerations uniquely applicable to Katakri and ISO/IEC 27000 ISMS standards, as well as some of the industry best practices. The diagram of the full process flow is presented in figure 12.

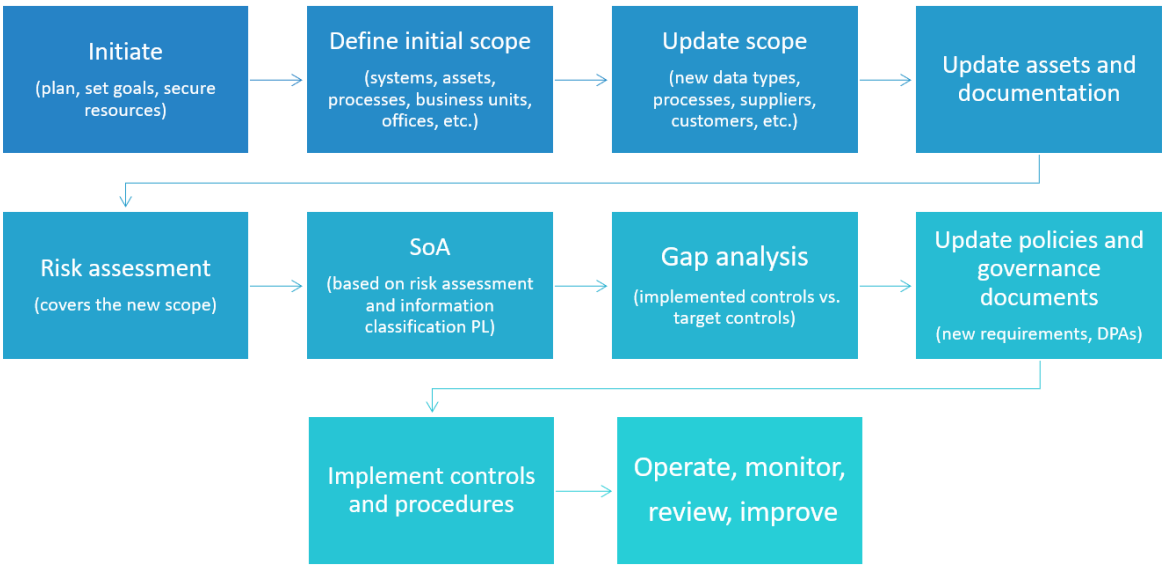

Figure 12. ISMS Enhancement Process for Reaching Compliance with Additional Security Requirements

Initiating the project involves the standard steps of securing managerial support, planning, and resourcing the project. New security goals are to be set for the ISMS, highlighting the desired state of compliance with the added security requirements framework.

When creating the scope statement, which addresses what, why, and from which treats the organisation should protect, it is important to remember that the scope of ISMS can vary between implementations in terms of processes, functions, services, locations, business units, administrative units, and suppliers included. Complying with multiple security requirements frameworks does not mean establishing multiple ISMS systems functioning simultaneously and independently from each other. It also does not mean scaling the implementation down, for instance, to one location to pass an audit on the local requirements. Aligning the ISMS with multiple frameworks almost always will lead to growing the scope of ISMS to include all the requirements. However, only the relevant parts of ISMS and security controls will be presented for evaluation during the audits. In other words, the scope of ISMS does not need to be the same as the scope of the pursued certification.

For example, if Company Y is ISO/IEC 27001 certified in its entirety, and only business unit A located on the territory of Finland provides services to the Finnish government and deals with the PII of Finnish citizens, assuming sufficient isolation between the business unit A and the rest of the company (e.g., network segmentation, firewalls, connection filters), business unit A and its subcontractors would need to be Katakri-certified and comply with the Act on the Personal Data Processing in the respective sector. Any IT and managerial functions that are involved in maintenance and administration of the business unit A

should also be included. Business units B and C do not need to be covered by the assessment. In this scenario, business unit A is still a part of the bigger ISMS and gets benefits from all the security measures already established for the ISO/IEC 27001 compliance. This scenario is visualised in figure 13.

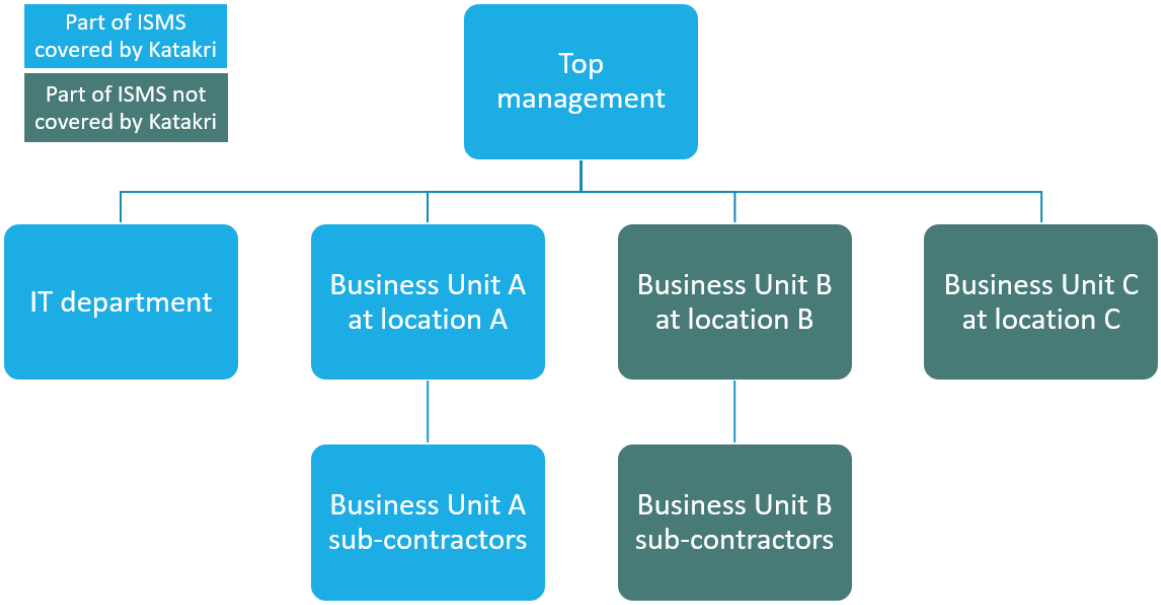

Figure 13. ISMS Certification Scope Example

After the general organisational scope covered by the new security requirements framework is determined, it makes sense to look at the assets in scope, evaluate the relevant inventory, and perform new risk analysis. In case of Katakri, at this stage an information classification must be introduced, and all the information assets in scope are to be labelled with the applicable protection level. An important consideration is the new types of data that might be processed as a result of reaching compliance. For example, if the Company Y needs to reach Katakri compliance to secure a contract with the Finnish government, will they also be processing PII of the Finnish citizens during this collaboration? If so, the data and parts of the system handling this data need to be classified accordingly. This would mean that some additional GDPR requirements must be implemented, such as Art. 24 on responsibilities of the data controller and Art. 28 on the responsibilities of the data processor (General Data Protection Regulation 2018). Data Protection Impact Assessment (DPIA) has to be developed for all cases of handling high-risk or high sensitivity information. Any subcontractors involved and getting access to the system data, for instance, when system maintenance is outsourced, are to be covered. Finally, the inventory of assets and documentation needs to be updated to reflect the new areas. These assets should also be covered by the risk analysis.

The next step is risk assessment. Unlike with ISO/IEC 27001, one cannot completely exclude some controls from their framework when implementing a Katakri-compliant system. In this case, the SoA will reflect how mature the controls need to be based on the results of the risk assessment of all the assets and processes in scope, as well as on the protection level of the information that is stored and handled within these assets and processes.

After the risk assessment, the team can look at the existing ISMS and security controls that are already implemented and perform the gap analysis to see which risks and requirements are already covered, and what enhancements are needed.

When relevant levels of security measures are identified and the gap analysis is conducted, information security policies and guidelines need to be updated to incorporate the new requirements. The security objectives also should be updated to reflect the new risks coming from new markets and clients that are the target audience of the systems in scope. Supplier relationships have to be re-evaluated at this point, and DPAs (Data Processing Agreement) with subcontractors need to be established or updated.

Next step is implementing controls and procedures. As suggested by the industry experts, for instance Irwin (27 July 2021), one way to ensure successful functioning of ISMS is to treat is as another project. It also helps to operationalize the ISMS by incorporating security procedures in the regular workflows (daily operations). This is supported by the fact that ISMS requirements implementation usually has a lot in common with a typical project work. Essentially, all implementation measures for the security controls need to specify what is to be done, what resources are required, who is responsible, when it is to be completed, and record evidence of how it was performed. Further on, monitoring and analysis of the performance is to be documented. An organisation can always choose to establish their own unique system for managing the ISMS. However, the required functionality is already widely available on the market in the form of the project management tools, specifically the ones focused on issue tracking. A common project and issue tracking tool Jira will be used here to provide an example of this approach.

Figure 14 presents a project dedicated to ISMS with the four components representing high-level focus areas identified during the security requirement frameworks analysis: technical, physical security, HR, and governance.

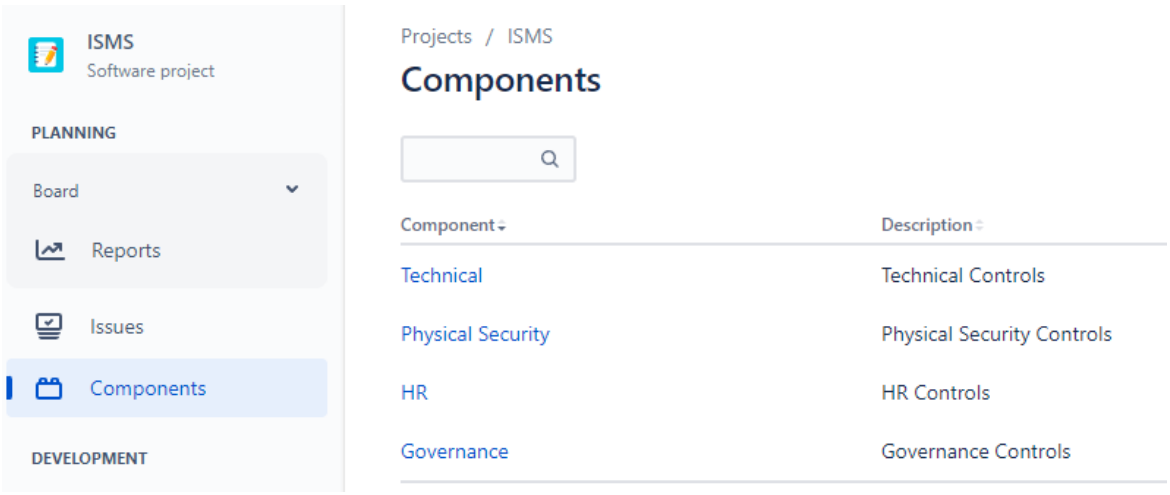

Figure 14. Example of a Jira Project Dedicated to ISMS and its Core Components

Figure 15 presents a sample of an ISMS control added to Jira as a ticket. It shows the project, control name, type (e.g., new feature, improvement, task, sub-task), control label, priority label, required procedures (sub-tasks), and the assigned task owner. It also shows the status of the sub-tasks related to this procedure.

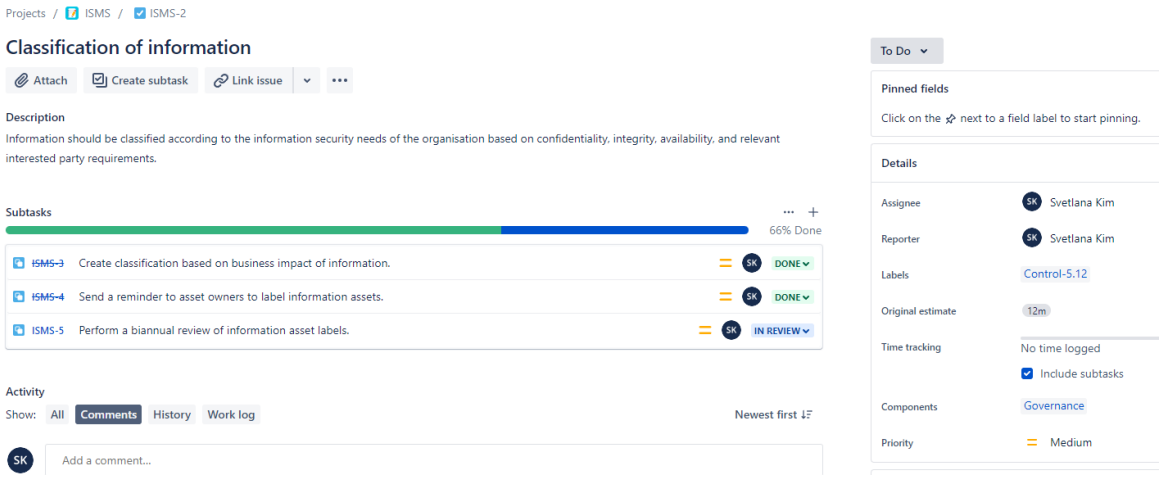

Figure 15. Example of a Jira Ticket Based on ISO/IEC 27002 Control 5.12

Likewise, all the other controls can be added as tickets with individual tasks. The tool also allows to set up automated reminders for the workflows. In addition, the tickets have an embed functionality for leaving comments, documenting change history, and work log. This allows to document, for instance, security incidents and response procedures, such as root cause analysis, fixes, follow-up procedures, evidence, communications, and incident response team members involved.

In a similar way, the ticketing system can also be used to maintain an inventory of assets and risks, especially when it comes to technology elements. Most ticketing systems allow to set up a custom status for the issue and label it with a priority and designated owner,

which is useful for asset and risk management. An example of the testing environment asset is presented in figure 16.

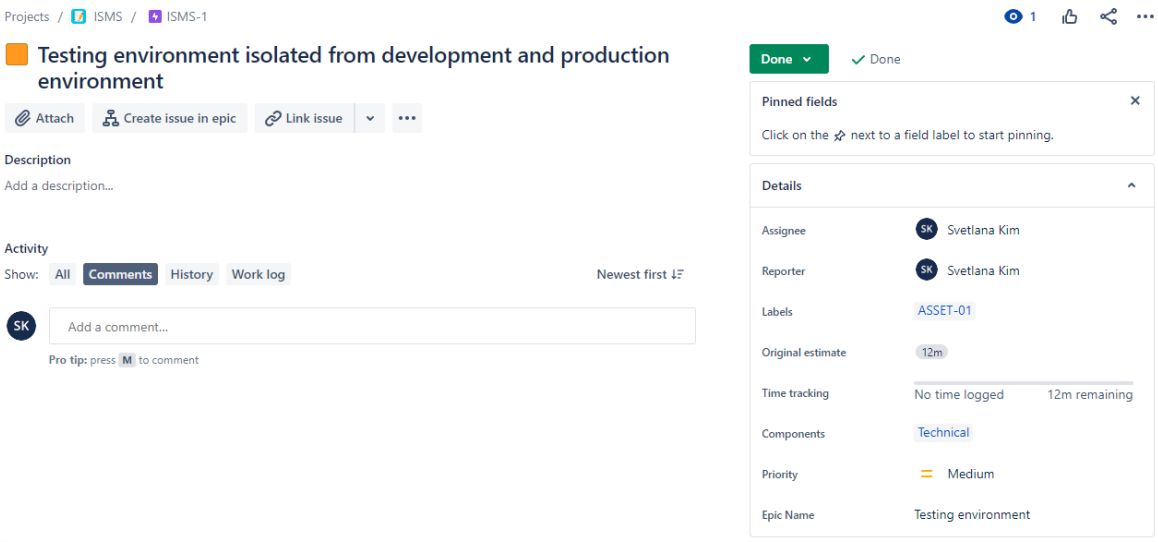

Figure 16. Example of a Jira Ticket for the Testing Environment Asset

There are many alternatives to the Jira software used for illustration purposes here. Some examples of the tools with similar functionality are Asana, Azure DevOps, GitHub Issues, Monday.com, and ClickUp (Atlassian s.a.). The implementation team can test the tools and see which one is the most convenient, provides best efficiency, and is suitable for their unique ways of working and type of services provided. Some tools might already be in use and familiar from other projects. In this case, it is easiest to just add another project dedicated to ISMS to the existing project management stock, rather than adopt a new dedicated tool.

Once all the new controls are implemented, the next stage is continuous ISMS operation, monitoring, evaluation, and improvement.

4.4 Additional Factors and Considerations

This section addresses some aspects that are important to consider when an organisation pursues compliance with the new information security regulations.

Firstly, if the new scope involves exploring new markets and migrating regions, it is important to look into the local legislation. For example, some countries (China, France, Germany, Indonesia, Russia, Vietnam) require that the servers storing their citizens' PII must be physically located on the territory of that country (Tolson 14 February 2019). To comply with this requirement, an organisation can consider subcontracting an CSP with the data centres located in that region.

In addition, for instance, Findata's regulation on the Requirements for other service providers' secure operating environments requires that the organisation must be registered on the territory of the EU (Findata 2022b, 14). This falls under the legislation category and is not in scope of this cybersecurity-focused approach to ISMS enhancement, an organisation would need to consult legal professionals to ensure compliance with this requirement.

Another important issue to consider is security clearances. In order to get access to and work with the Classified Information, organisation's employees might need to go through the procedure of security clearance conducted by the governmental representative bodies or other entities approved by the authorities in cooperation with the local law enforcement agencies. In Finland, security clearances are provided by Supo (Suojelupoliisi), the Finnish Security and Intelligence Service (Supo s.a.). Supo performs a background check on the person and provides the results to the requesting organisation in the form of a generalised conclusion on the propriety of person's access to the information in question. Security clearance can be obtained only for relevant purposes, and not all categories of classified information require security clearance to get access. In many cases employee's trustworthiness and reliability can be ensured with compensatory measures, such as proper identity verification, comprehensive training, exhaustive company information security policies, and NDA / Confidentiality Agreement in place.

4.5 Importance and Benefits of ISMS Assessment and Certification

To enable continual improvement of ISMS, it is necessary to assess its performance and identify improvement areas. It is recommended to perform the regular review of ISMS performance results annually or bi-annually with a few periodic (for instance, quarterly) reviews in between. Top management should be involved in the reviews and decision-making process.

Additionally, the certifications have a fixed validity period. For example, the validity period of ISO/IEC 27001 compliance certification is 3 years, meaning that the entire ISMS needs to be reassessed every third year to maintain the certified status. The cycle of certification maintenance audits is presented on figure 17. The annual external surveillance audits are also performed to verify the system's capability to maintain the performance and operate as intended, organisation's adherence to the outlined procedures, that the deficiencies identified in the previous year have been fixed, and that the system is continually improved. During the surveillance audit, only some areas of ISMS are tested. Specifically,

the operational procedures can be tested with a multi-sample evidence, and the areas that experienced significant changes or updates since the last audit need to be re-evaluated.

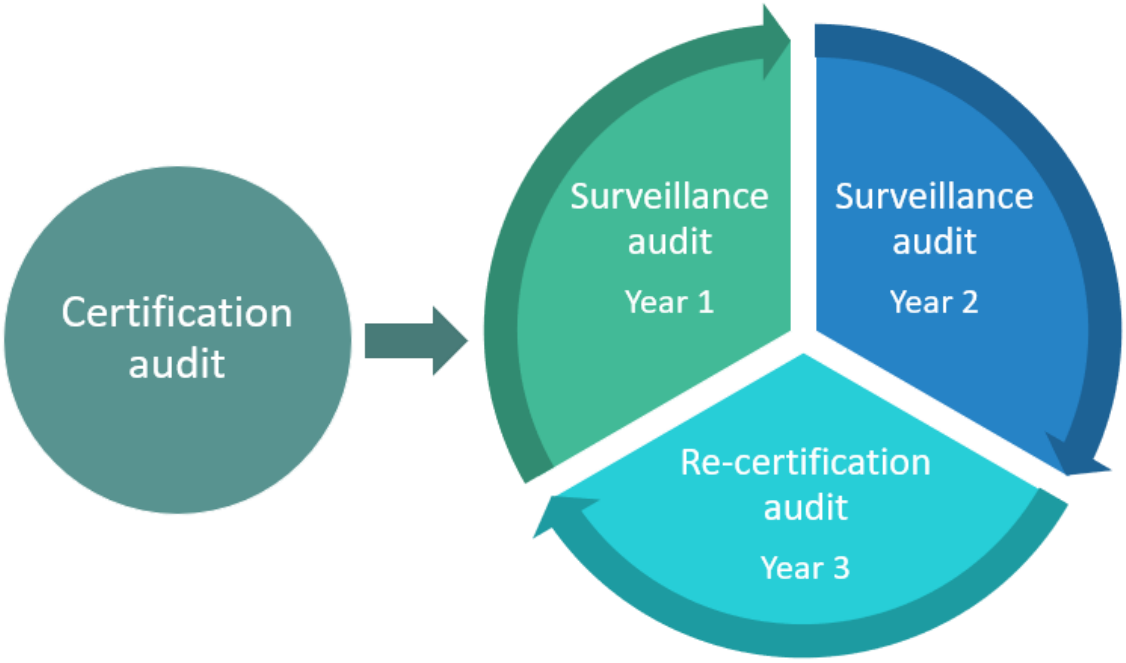

Figure 17. ISMS Certification Maintenance Audits Cycle

The requirements to the certification bodies verifying compliance with ISO/IEC 27001 are presented in the ISO/IEC 27006 standard (2015) and the guidance for ISMS audit is provided in the ISO/IEC 27007 standard (2020). ISO/IEC 27006 supplements ISO/IEC 17021, “Conformity assessment – Requirements for bodies providing audit and certification of management systems” (2015). It is mandatory to comply with the requirements of this standard, demonstrating competence and reliability, in order to obtain accreditation and be able to provide consistent evaluation against the ISO/IEC 27001 requirements.

Katakri has the guidance on assessment of information security systems attached in Appendix II. The assessment process is recommended to be used for the internal audit. The same appendix also contains information about obtaining accreditation from Traficom. The validity of Katakri accreditation expires after three years or upon significant changes affecting the security of the inspection target. Annex III contains additional information regarding security assessment based on Katakri Security Model, a hybrid model covering the minimum requirements adjustable based on risk analysis. The goal of the minimum requirements is to mitigated common risks related to Classified Information. Both processes are presented in figure 18.

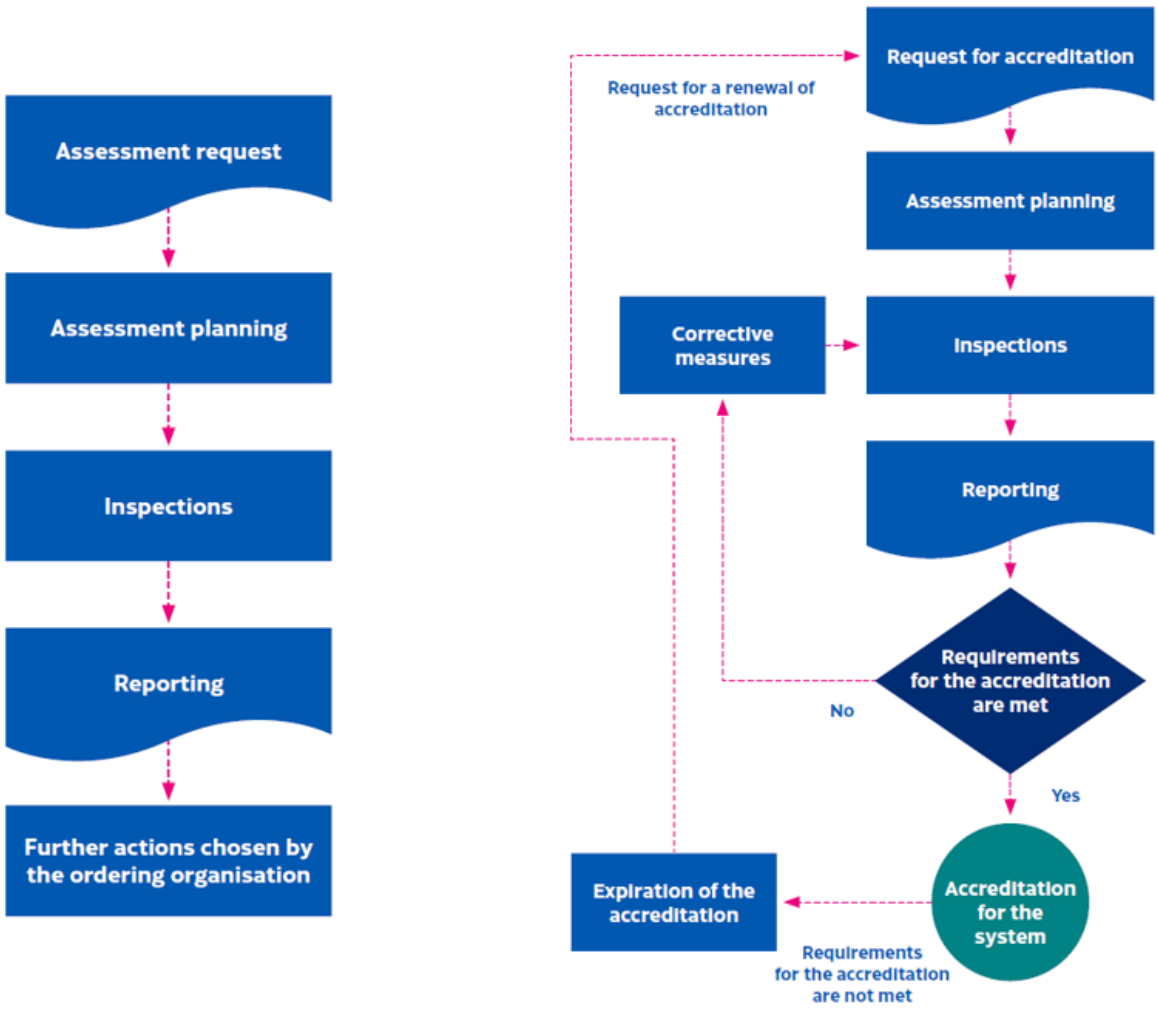

Figure 18. Katakri assessment and accreditation processes (National Security Authority of Finland 2020, 111-112)

A certified ISMS demonstrates organisation's commitment to information security and provides assurance to the authorities, customers, and stakeholders. Getting the ISMS audited by an independent assessment body and certified:

- Facilitates compliance with legal requirements and helps to avoid associated fines.
- Protects organisation from the common risks.
- Provides external review that can reveal deficiencies and vulnerabilities in the system that need to be fixed.
- Improves security and minimizes the chance of incidents due to thorough examination and testing.
- Establishes a consistent process of monitoring the state of information security in the organisation.
- Supports and protects organisation's reputation.

- Gives competitive advantage on the market and reduces resources required to prove organisation's robust risk management and information security approach when entering contractual relationships with the new customers and business partners.
- Helps to meet customer expectations regarding quality of the delivered services.

Internal audit can be performed by a team of independent internal experts or by external consultants hired for this purpose. The benefit of external consultant in this case is that an organisation gets outside view and recommendations from an experienced professional who had worked with multiple similar projects. The internal audit is needed to perform a routine review of the system's operations, identify possible deficiencies, and fix them. It also helps to prepare for the external audits. Clause 9.2 of ISO/IEC 27001 (2013, 8) states that the purpose of regular internal audit is to provide information on whether the ISMS conforms to organisation's own requirements, requirements of the standard, and whether it is effectively implemented and maintained. The results of the internal audit are reported to the top management to determine whether the set objectives are met, and changes and improvements are needed.

There are many benefits to the internal audit, but it should be periodic, as some experts note a phenomenon known as "audit fatigue" (Zhao 2022). When the internal and external audits are conducted too often, the organisation ends up in an endless cycle of inspections, interviews, collecting evidence, and assessments. As much as the review of one's work is important, when it is performed continually employees get exhausted by the bureaucratic aspect. It also takes a lot of time and distracts from performing other duties. Thus, it is vital to minimize the impact of the audit activities on the daily operations.

5 Discussion

The purpose of the research was to examine common information security standards, regulations, and frameworks, to perform comparative analysis of the requirements laid out on the international and national level, and to propose a strategic approach to ISMS enhancement with the goal of reaching compliance with additional regional requirements.

Achieved objectives

The objectives that were set at the beginning of this research, and were successfully complete, include:

1) Built a theoretical framework covering the concepts of ISMS, cybersecurity strategy, and risk management. The explored topics are:
- risk analysis and evaluation
- ISMS purpose, benefits, and structural components
- common challenges with implementing and operating an ISMS
- ISMS lifecycle
- additional factors, such as business context, company culture, top management involvement, resources, awareness, and HR-related issues.

2) Examined the common international (ISO/IEC 27000 series, ISO/IEC 15408 Common Criteria, GDPR, NIST CSF) and national (VAHTI, Katakri, PiTuKri, Kanta, Findata) cybersecurity requirement frameworks.
3) Conducted comparative analysis of the international information security standard ISO/IEC 27002:2022 against the national Katakri 2020 information security criteria.
4) Proposed a strategic project-based approach to implementing enhancement changes necessary to reach compliance with additional security requirements.

Research results

Comparative analysis of ISO/IEC 27002:2022 and Katakri 2020 revealed a number of common security areas comprising the baseline information security benchmark. These areas include governance, physical security (of premises and assets), personnel security, and technical security (software, network, digital data, operations, connections). Both frameworks allow for some flexibility in regard to the implementation measures depending on the level of protection needed based on risk analysis and business-specific impact evaluation.

There were also identified some fundamental differences between the frameworks. Namely, the focus areas: Katakri aims at protection of classified information, while

ISO/IEC 27000 series are aimed at effective ISMS implementation protecting organisation's systems and business data. The difference in scope is also evident. As Katakri is a security audit tool, it provides assessment criteria for the implemented system, but not the requirements for system development or testing. Cloud services are not covered by Katakri either, while the newest version of ISO/IEC 27002 includes a clause on security of cloud services.

In general, compliance with either framework provides a certain level of assurance regarding information security in the organisation. The security requirements of the frameworks can be relatively easily combined within an ISMS implementation for additional protection and regional compliance. The proposed strategic approach to such ISMS enhancement involves step-by-step analysis, development, and implementation process with the project-based structure.

Challenges

The first challenge was getting access to some of the standards. For example, ISO/IEC 27000 series are not available in open access. The access can only be obtained through purchasing a personal use license or being affiliated with an accredited certification body. It was possible to obtain copies for personal learning purposes due to the professional activities as a cyber security specialist.

It also proved to be quite challenging to establish direct and indirect correlations between ISO/IEC 27002 and Katakri. It would be beneficial to support this study with a quantitative correlation analysis, however, due to differences in terminology and focus areas, it was not possible to achieve at this stage. Contextual qualitative analysis was successfully performed and revealed multiple correlations.

Learning Outcomes

As a result of the study, a number of learning objectives were reached:

- improved understanding of cybersecurity facilitating professional development
- studied international and Finland's national cybersecurity practices
- built a substantial knowledge applicable in daily work
- built a comprehensive document base regarding ISMS and information security frameworks.

Timeline

Thesis project and research work was mostly performed between March and May 2022.

Further Development

There is a lot of space for further research of cybersecurity frameworks, specifically the national ones, such as PiTuKri dedicated to the cloud services. International organisations that want to enter Finland's market would also benefit from the research on national legislation and regulations concerning personal data of Finnish citizens.

Applicability of the results

The results of the research can be utilized by organisations who want to improve their ISMS and reach compliance with new regulations. The study is also relevant for anyone who is interested in cybersecurity and developing general knowledge about securing business operations and data. In addition, the comprehensive overview of commonly applied requirements can be helpful for anyone who wants to understand the differences between approaches and frameworks.

References

Act on the Secondary Use of Health and Social Data (552/2019).

Abuhav, I. 2014. The Plan Do Check Act (PDCA) cycle. URL: http://9001quality.com/plan-do-check-act-pcda-iso-9001/. Accessed: 16 April 2022.

Alan Calder, S. W. 2019. Information Security Risk Management for ISO 27001/ISO 27002, third edition. IT Governance Publishing.

Alexander, D., Finch, A., Sutton, D. & Taylor, A. 2013. Information Security Management Principles. 2. Swindon: BCS Learning & Development Limited.

Atlassian s.a. Jira Software Alternatives. URL: https://www.atlassian.com/software/jira/comparison. Accessed: 11 May 2022.

Chopra, A. & Chaudhary, M. 2020. Implementing an Information Security Management System: Security Management Based on ISO 27001 Guidelines. Apress.

Digital and Population Data Services Agency 2020. VAHTI-instructions. URL: https://www.suomidigi.fi/en/ohjeet-ja-tuki/vahti-instructions. Accessed: 2 May 2022.

Dutton, J. 4 June 2019. What is an ISMS? 9 reasons why you should implement one. IT Governance Blog. URL: https://www.itgovernance.co.uk/blog/what-is-an-isms-and-9-reasons-why-you-should-implement-one. Accessed: 13 April 2022.

Findata, Finnish Social and Health Data Permit Authority 2022a. Regulation 1/2022. Regulation by the Health and Social Data Permit Authority: Requirements for other service providers' secure operating environment.

Findata, Finnish Social and Health Data Permit Authority 2022b. Regulation 1/2022. Annex 1: Requirements for a Secure Operating Environment.

General Data Protection Regulation 2018. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. URL: https://gdprinfo.eu/. Accessed: 4 May 2022.

IEC 2022. Electropedia: The World's Online Electrotechnical Vocabulary. URL: https://www.electropedia.org/. Accessed: 11 May 2022.

Irwin, L. 27 July 2021. How to implement and maintain an ISO 27001-compliant ISMS. IT Governance Blog. URL: https://www.itgovernance.eu/blog/en/how-to-implement-an-isms-aligned-with-iso-27001-2. Accessed: 12 May 2022.

ISO 2022a. Online Browsing Platform (OBP) Version 4.19.0. URL: https://www.iso.org/obp/ui#home. Accessed: 11 May 2022.

ISO 2022b. Standards by ISO/IEC JTC 1/SC 27 - Information security, cybersecurity and privacy protection. URL: https://www.iso.org/committee/45306/x/catalogue/. Accessed: 3 May 2022.

ISO 31000:2018. Risk management — Guidelines.

ISO/IEC 27000:2018. Information technology – Security techniques – Information security management systems – Overview and vocabulary.

ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements.

ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection – Information security controls.

ISO/IEC 27003:2017. Information technology – Security techniques – Information security management systems – Guidance.

ISO/IEC 27004:2016. Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation.

ISO/IEC 27005:2018. Information technology – Security techniques – Information security risk management.

ISO/IEC 27006:2015. Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems.

ISO/IEC 27007:2020. Information security, cybersecurity and privacy protection – Guidelines for information security management systems auditing.

Jucan, M. 5 September 2016. Top challenges faced by information security teams implementing ISO 27001. IT Governance Blog. URL: https://www.itgovernanceusa.com/blog/top-challenges-faced-by-information-security-teams-implementing-iso-27001. Accessed: 13 April 2022.

Kanta Services, The Social Insurance Institution of Finland 1 November 2021. Legislation. URL: https://www.kanta.fi/en/legislation. Accessed: 3 May 2022.

Kirvan, P. & Granneman, J. 2021. Top 10 IT security frameworks and standards explained. TechTarget. URL: https://www.techtarget.com/searchsecurity/tip/IT-security-frameworks-and-standards-Choosing-the-right-one. Accessed: 30 April 2022.

Kosutic, D. 14 July 2014. How to maintain the ISMS after the certification. Advisera Expert Solutions Blog. URL: https://advisera.com/27001academy/blog/2014/07/14/how-to-maintain-the-isms-after-the-certification/. Accessed: 21 April 2022.

Kosutic, D. s.a. ISO 27001 Implementation Guide: Checklist of Steps, Timing, and Costs involved. Advisera Expert Solutions Knowledgebase. URL: https://advisera.com/27001academy/knowledgebase/iso-27001-implementation-checklist/. Accessed: 20 April 2022.

Mead, N. 2013. The Common Criteria. Carnegie Mellon University 2005-2012. URL: https://www.cisa.gov/uscert/bsi/articles/best-practices/requirements-engineering/the-common-criteria. Accessed: 6 May 2022.

Mooney, T. 2015. Information Security a Practical Guide: Bridging the gap between IT and management. IT Governance Ltd.

Mutune, G. 2019. 23 Top Cybersecurity Frameworks. URL: https://cyberexperts.com/cybersecurity-frameworks/. Accessed: 1 May 2022.

National Institute of Standards and Technology 2014. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.0.

National Security Authority of Finland 2020. Katakri – Information Security Audit Tool for Authorities.

Patel, R. 28 March 2021. Introduction to Information Security Management Systems (ISMS) and Implementation Procedure. URL: https://www.linkedin.com/pulse/introduction-information-security-management-systems-isms-patel/. Accessed: 10 April 2022.
Schou, C., Faber, F., Hernandez, S. & Slay, J. 2014. Information Assurance Handbook: Effective Computer Security and Risk Management Strategies. New York: McGraw-Hill.

Sharron, M. 2022. ISO 27001 Implementation – 4 Key Challenges & How to Overcome Them. URL: https://www.isms.online/iso-27001/iso-27001-implementation-4-key-challenges-how-to-overcome-them/. Accessed: 13 April 2022.

Sullivan, M. 18 March 2022. How to avoid GDPR fines in 2022 (plus the 3 largest GDPR fines to date). Transcend Blog. URL: https://transcend.io/blog/gdpr-fines/. Accessed: 27 April 2022.

Supo, Finnish Security and Intelligence Service s.a. About Supo. URL: https://supo.fi/en/about-supo. Accessed: 11 May 2022.

The Security Committee 2019. Finland's Cyber Security Strategy 2019. Government Resolution 3.10.2019.

Tolson, B. 14 February 2019. What is Data Sovereignty and the GDPR: Do You Know Where Your Data is Located? Archive360 Blog. URL: https://www.archive360.com/blog/data-sovereignty-and-the-gdpr-do-you-know-where-your-data-is. Accessed: 11 May 2022.

Traficom Finnish Transport and Communications Agency, National Cyber Security Centre 2020. Criteria to Assess the Information Security of Cloud Services (PiTuKri). Traficom publications 20/2020. PiTuKri – version 1.1 – March 2020.

Turvallisuuskomitea Puolustusministeriö s.a. Security Committee. URL: https://turvallisuuskomitea.fi/en/security-committee/. Accessed: 1 May 2022.

Valvira, National Supervisory Authority for Welfare and Health 2022. Social welfare and healthcare data systems. URL: https://www.valvira.fi/web/en/healthcare/social-welfare-and-healthcare-data-systems. Accessed: 15 May 2022.

Van Otterloo, S. 2017. Information security and PDCA (Plan-Do-Check-Act). ICT Institute. URL: https://ictinstitute.nl/pdca-plan-do-check-act/. Accessed 23 April 2017.

Wolford, B. s.a.-a. What are the GDPR Fines? GDPR.EU. URL: https://gdpr.eu/fines/. Accessed: 27 April 2022.

Wolford, B. s.a.-b. What is GDPR, the EU’s new data protection law? GDPR.EU. URL: https://gdpr.eu/what-is-gdpr/. Accessed: 30 April 2022.

Wright, C. 2008. The IT Regulatory and Standards Compliance Handbook. Syngress.

Zhao, J. 2022. How to Reduce Audit Fatigue and Compliance Costs (Tips from Security Professionals). URL: https://hyperproof.io/resource/audits-fatigue/. Accessed: 15 May 2022.

List of Other Sources

This section provides the list of sources that are not directly referenced in the work but were studied during the research and deemed relevant. They have influenced some general ideas and promoted the research. These sources might present interest for anyone who would want to look further into the topic of information security.

AICPA 2020. 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy. URL: https://us.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf. Accessed: 1 May 2022.

Alan Calder, S. W. 2021. ISO 27001 ISMS Lead Implementer Training Course. IT Governance Publishing.

Alliantist Ltd s.a. ISMS Business Case Builder – Understanding the Components of an ISMS Solution. URL: https://www.isms.online/isms-business-case-builder/components-of-an-isms/. Accessed: 17 April 2022.

Gantz, S. D. & Maske, S. 2013. The Basics of IT Audit. Syngress.

NIST s.a. Cybersecurity Framework. URL: https://www.nist.gov/cyberframework. Accessed: 30 March 2022.

Ministry of Finance s.a. Digital security: Guidance of services and security. URL: https://vm.fi/en/information-security-and-cybersecurity. Accessed: 27 March 2022.

Wheeler, E. & Swick, K. 2011. Security Risk Management. Syngress.

Appendices

Appendix 1. Abbreviations

2FA	Two-Factor Authentication
AES	Advanced Encryption Standard
AD	Active Directory
AICPA	Association of International Certified Professional Accountants
AV	Antivirus
BCP	Business Continuity Plan
BYOD	Bring Your Own Device
CC	Common Criteria
CEM	Common Evaluation Methodology
CIA	Confidentiality, Integrity, Availability
CISO	Chief Information Security Officer
CIS	Center for Internet Security
CSP	Cloud Service Provider
CSF	Cyber Security Framework
DLP	Data Loss Prevention
DPA	Data Processing Agreement
DPIA	Data Protection Impact Assessment
EAL	Evaluation Assurance Level
EU	European Union
FISMA	Federal Information Security Management Act
GDPR	General Data Protection Regulation
HIPAA	The Health Insurance Portability and Accountability Act
HR	Human Resources
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
ISMS	Information Security Management System
ISO	International Organisation for Standardization
ISRM	Information Security and Risk Management
IT	Information Technology
Katakri	Kansallinen turvallisuusauditointikriteeristö, Information Security Audit Tool for Authorities
KPI	Key Performance Indicator
LAN	Local Area Network

MFA	Multi-Factor Authentication
NDA	Non-disclosure agreement
NIST	National Institute of Standards and Technology (of U.S.A.)
NSA	National Security Authority of Finland
OS	Operating System
OWASP	Open Web Application Security Project
PaaS	Platform as a Service
PCI DSS	Payment Card Industry Data Security Standard
PDCA	Plan-Do-Check-Act
PII	Personally Identifiable Information
PL	Protection Level
PP	Protection Profile
QA	Quality Assurance
RFP	Request for Proposal
SaaS	Software as a Service
SIEM	Security Information and Event Management
SLA	Service-Level Agreement
SoA	Statement of Applicability
SOC	System and Organisation Controls
Supo	Suojelupoliisi, The Finnish Security and Intelligence Service
TOE	Target of Evaluation
Traficom	Finnish Transport and Communications Agency
TSC	Trust Services Criteria
UPS	Uninterruptible Power Supply
VPN	Virtual Private Network

Appendix 2. ISO/IEC 27000 Series Standards

Table 5. List of the main published and currently being developed standards from the ISO/IEC 27000 Series (adapted from ISO 2022b)

Standard	Published	Title
ISO/IEC 27000	2018	Information technology – Security techniques – Information security management systems – Overview and vocabulary
ISO/IEC 27001	2013	Information technology – Security techniques – Information security management systems – Requirements
ISO/IEC 27002	2022	Information security, cybersecurity and privacy protection – Information security controls
ISO/IEC 27003	2017	Information technology – Security techniques – Information security management systems – Guidance
ISO/IEC 27004	2016	Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation
ISO/IEC 27005	2018	Information technology – Security techniques – Information security risk management
ISO/IEC 27006	2015	Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems
ISO/IEC 27007	2020	Information security, cybersecurity and privacy protection – Guidelines for information security management systems auditing
ISO/IEC TS 27008	2019	Information technology – Security techniques – Guidelines for the assessment of information security controls
ISO/IEC 27009	2020	Information security, cybersecurity and privacy protection – Sector-specific application of ISO/IEC 27001 – Requirements
ISO/IEC 27010	2015	Information technology – Security techniques – Information security management for inter-sector and inter-organisational communications
ISO/IEC 27011	2016	Information technology – Security techniques – Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organisations
ISO/IEC 27013	2021	Information security, cybersecurity and privacy protection – Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

ISO/IEC 27014	2020	Information security, cybersecurity and privacy protection – Governance of information security
ISO/IEC TR 27016	2014	Information technology – Security techniques – Information security management – Organisational economics
ISO/IEC 27017	2015	Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services
ISO/IEC 27018	2019	Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
ISO/IEC 27019	2017	Information technology – Security techniques – Information security controls for the energy utility industry
ISO/IEC 27021	2017	Information technology – Security techniques – Competence requirements for information security management systems professionals
ISO/IEC TS 27022	2021	Information technology – Guidance on information security management system processes
ISO/IEC TR 27023	2015	Information technology – Security techniques – Mapping the revised editions of ISO/IEC 27001 and ISO/IEC 27002
ISO/IEC AWI TR 27024	Under development	ISO/IEC 27001 family of standards references list – Use of ISO/IEC 27001 family of standards in Governmental / Regulatory requirements
ISO/IEC 27031	2011	Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity
ISO/IEC 27032	2012	Information technology – Security techniques – Guidelines for cybersecurity
ISO/IEC 27037	2012	Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence
ISO/IEC 27038	2014	Information technology – Security techniques – Specification for digital redaction
ISO/IEC 27039	2015	Information technology – Security techniques – Selection, deployment and operations of intrusion detection and prevention systems (IDPS)
ISO/IEC 27040	2015	Information technology – Security techniques – Storage security

ISO/IEC 27041	2015	Information technology – Security techniques – Guidance on assuring suitability and adequacy of incident investigative method
ISO/IEC 27042	2015	Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence
ISO/IEC 27043	2015	Information technology – Security techniques – Incident investigation principles and processes
ISO/IEC 27070	2021	Information technology – Security techniques – Requirements for establishing virtualized roots of trust
ISO/IEC FDIS 27099	Under development	Information Technology – Public key infrastructure – Practices and policy framework
ISO/IEC TS 27100	2020	Information technology – Cybersecurity – Overview and concepts
ISO/IEC 27102	2019	Information security management – Guidelines for cyber-insurance
ISO/IEC TR 27103	2018	Information technology – Security techniques – Cybersecurity and ISO and IEC Standards
ISO/IEC AWI TR 27109	Under development	Cybersecurity education and training
ISO/IEC TS 27110	2021	Information technology, cybersecurity and privacy protection – Cybersecurity framework development guidelines
ISO/IEC 27400	Under development	Cybersecurity – IoT security and privacy – Guidelines
ISO/IEC CD 27403	Under development	Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics
ISO/IEC TR 27550	2019	Information technology – Security techniques – Privacy engineering for system life cycle processes
ISO/IEC 27551	2021	Information security, cybersecurity and privacy protection – Requirements for attribute-based unlinkable entity authentication
ISO/IEC CD 27554	Under development	Application of ISO 31000 for assessment of identity-related risk
ISO/IEC 27555	2021	Information security, cybersecurity and privacy protection – Guidelines on personally identifiable information deletion

ISO/IEC DIS 27556	Under development	Information security, cybersecurity and privacy protection – User-centric privacy preferences management framework
ISO/IEC DIS 27557	Under development	Information technology – Information security, cybersecurity and privacy protection – Organisational privacy risk management
ISO/IEC DIS 27559	Under development	Privacy enhancing data de-identification framework
ISO/IEC AWI TS 27560	Under development	Privacy technologies – Consent record information structure
ISO/IEC AWI 27561	Under development	Information technology – Security techniques – Privacy operationalisation model and method for engineering (POMME)
ISO/IEC AWI 27562	Under development	Security and privacy in artificial intelligence use cases
ISO/IEC DTR 27563	Under development	Impact of security and privacy in artificial intelligence
ISO/IEC AWI 27565	Under development	Guidelines on privacy preservation based on zero knowledge proofs
ISO/IEC TS 27570	2021	Privacy protection – Privacy guidelines for smart cities
ISO/IEC 27701	2019	Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines

Appendix 3. ISO/IEC 27002:2022 Standard – Controls

Table 6. Full List of Controls from ISO/IEC 27002:2022 Standard (ISO/IEC 2022)

Identifier	Control Name
5	Organisational controls
5.1	Policies for information security
5.2	Information security roles and responsibilities
5.3	Segregation of duties
5.4	Management responsibilities
5.5	Contact with authorities
5.6	Contact with special interest groups
5.7	Threat intelligence
5.8	Information security in project management
5.9	Inventory of information and other associated assets
5.10	Acceptable use of information and other associated assets
5.11	Return of assets
5.12	Classification of information
5.13	Labelling of information
5.14	Information transfer
5.15	Access control
5.16	Identity management
5.17	Authentication information
5.18	Access rights
5.19	Information security in supplier relationships
5.20	Addressing information security within supplier agreements
5.21	Managing information security in the ICT supply chain
5.22	Monitoring, review and change management of supplier services
5.23	Information security for use of cloud services
5.24	Information security incident management planning and preparation
5.25	Assessment and decision on information security events
5.26	Response to information security incidents
5.27	Learning from information security incidents
5.28	Collection of evidence
5.29	Information security during disruption
5.30	ICT readiness for business continuity
5.31	Legal, statutory, regulatory and contractual requirements
5.32	Intellectual property rights
5.33	Protection of records

5.34	Privacy and protection of PII
5.35	Independent review of information security
5.36	Compliance with policies, rules and standards for information security
5.37	Documented operating procedures
6	People controls
6.1	Screening
6.2	Terms and conditions of employment
6.3	Information security awareness, education and training
6.4	Disciplinary process
6.5	Responsibilities after termination or change of employment
6.6	Confidentiality or non-disclosure agreements
6.7	Remote working
6.8	Information security event reporting
7	Physical controls
7.1	Physical security perimeters
7.2	Physical entry
7.3	Securing offices, rooms and facilities
7.4	Physical security monitoring
7.5	Protecting against physical and environmental threats
7.6	Working in secure areas
7.7	Clear desk and clear screen
7.8	Equipment siting and protection
7.9	Security of assets off-premises
7.10	Storage media
7.11	Supporting utilities
7.12	Cabling security
7.13	Equipment maintenance
7.14	Secure disposal or re-use of equipment
8	Technological controls
8.1	User endpoint devices
8.2	Privileged access rights
8.3	Information access restriction
8.4	Access to source code
8.5	Secure authentication
8.6	Capacity management
8.7	Protection against malware
8.8	Management of technical vulnerabilities

8.9	Configuration management
8.10	Information deletion
8.11	Data masking
8.12	Data leakage prevention
8.13	Information backup
8.14	Redundancy of information processing facilities
8.15	Logging
8.16	Monitoring activities
8.17	Clock synchronization
8.18	Use of privileged utility programs
8.19	Installation of software on operational systems
8.20	Networks security
8.21	Security of network services
8.22	Segregation of networks
8.23	Web filtering
8.24	Use of cryptography
8.25	Secure development life cycle
8.26	Application security requirements
8.27	Secure system architecture and engineering principles
8.28	Secure coding
8.29	Security testing in development and acceptance
8.30	Outsourced development
8.31	Separation of development, test and production environments
8.32	Change management
8.33	Test information
8.34	Protection of information systems during audit testing

Appendix 4. Katakri 2020 – Requirements

Table 7. Full List of Requirements from Katakri 2020 Information Security Audit Tool for Authorities (National Security Authority of Finland 2020)

Identifier	Requirement Name
T-01	Support from the management, guidance, responsibilities – Security principles
T-02	Defining the tasks and responsibilities of the security management
T-03	Management of information security risks
T-04	Security guidance
T-05	Resources for the security work
T-06	Malfunctions and exceptional situations
T-07	Management of security events
T-08	Classification of information
T-09	Changes in the handling of classified information throughout the employment
T-10	Assessment of the trustworthiness and reliability of the personnel
T-11	Non-disclosure and confidentiality commitment
T-12	Security education
T-13	Need-to-know and access rights
F-01	Goal for physical security measures
F-02	Risk assessment of physical security measures
F-03	Selection of physical security measures (defence-in-depth)
F-04	Handling and storage of information in security areas and outside
F-05	Administrative area
F-05.1	Boundary and structures for the area (walls, doors, windows, floor and ceiling structures)
F-05.2	Management of access rights
F-05.3	Visitors
F-05.4	Soundproofing
F-05.5	Intrusion detection systems
F-05.6	Protection from unauthorized observation
F-05.7	Inspections of working spaces and devices (only for national classification level II or EU secret)
F-05.8	Handling and storage of information
F-06	Secured area
F-06.1	Boundary and structures for the area (walls, doors, windows, floor and ceiling structures)

F-06.2	Access control
F-06.3	Management of access rights
F-06.4	Visitors
F-06.5	Security instructions
F-06.6	Soundproofing
F-06.7	Intrusion detections systems
F-06.8	Protection from unauthorized observation
F-06.9	Inspections of working spaces and devices (only for national classification level II or EU secret)
F-06.10	Handling and storage of information
F-07	Technically secured area
F-08	Data security
F-08.1	Transfer of information by using postal or courier services
F-08.2	Copying of classified information
F-08.3	Registering of classified information
F-08.4	Disposal of information in non-electronic format
I-01	Secure interconnection of CIS – Security of the network architecture
I-02	Principle of least privilege – Segmenting of the communication network and filtering rules within the classification level
I-03	Security of information processing environment throughout the life cycle – Management of filtering and monitoring systems
I-04	Secure interconnection of CIS – Management connections
I-05	Exchange of classified information outside the physically protected areas – Wireless transmission
I-06	The principle of least privilege – Management of access rights
I-07	Defence-in-depth – Identification of actors of the information processing environment within a physically protected security area
I-08	Principle of minimality and of least privilege – Systems hardening
I-09	Defence-in-depth – Protection against malware
I-10	Defence in depth – Traceability of security events
I-11	Defence-in-depth – Incident detection and recovery
I-12	Evaluation and approval of cryptographic products – Crypto solutions
I-13	Defence-in-depth throughout the life cycle – Protection of software against network attacks
I-14	Defence-in-depth – Electromagnetic emanations (TEMPEST) and electronic intelligence
I-15	Exchange of classified information between physically protected areas – Electronic transfer of the information

I-16	Security throughout the information processing Environment life cycle – change management
I-17	Handling of classified information within physically protected areas – Physical security
I-18	Handling and transfer of classified information between physically protected areas – Remote use and remote management
I-19	Security throughout the information processing environment lifecycle – Management of software vulnerabilities
I-20	Security throughout the information processing environment lifecycle – Backup copies
I-21	Security throughout the information processing environment lifecycle – Disposal of classified information in electronic format