jamk

Preparing DevOps for ISO 27001 certification

Marjo Laine

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

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Description

Laine, Marjo

Preparing DevOps for ISO 27001 certification

Jyväskylä: Jamk University of Applied Sciences, November 2024, 64 pages

Degree Programme in Cyber Security. Master's thesis.

Permission for open access publication: Yes

Language of publication: English

Abstract

In modern software development, and IT industry in general, the need for information security assurance is increasing by the day. ISO 27001 is well known and the current de facto information security standard and getting certified has many benefits from minimizing the risk of information security incidents to increasing customer trust and sales. The thesis sought to answer the question of how a small to medium sized software company can prepare their DevOps functions for ISO 27001 certification.

The thesis was split into three parts and sub questions. First ISO 27001 standard's Annex A was reviewed, and controls related to DevOps were identified and listed followed by a literary review of different online sources to find the best practices and recommendations related to these ISO 27001 controls to answer the sub questions of how a company's current situation can be mapped out and what kind of best practices should be in place to become certified. The last sub question was how to implement the recommendations and thus the last part is a practical section of making the improvements. All of these findings were applied at the same time to Company X, a medium-sized software company, and their environment was used in the last part as an example on the parts where publishing was possible. The actions made in Company X are included in appendixes that were made confidential.

The result was a theoretical and in-practice step-by-step guide for DevOps teams in small to medium software businesses on how to improve their security posture following ISO 27001 best practices whether the goal is to become certified or just doing things in a more secure way. However, the thesis did not become a complete guide as some bigger topics, like creating continuity plans, had to be left out due to the size of the task and/or because they required company-wide decision making. In addition to the actual guide, it was found out how much becoming certified or compliant with any information security framework is a team effort of the whole company, not just technical staff, and that management blessing is crucial for success.

Keywords/tags (subjects)

DevOps, DevSecOps, ISO 27001, Software Development, Compliance, Information Security, Small to Medium Businesses, Compliance, Information Security Management System (ISMS), Certification

Miscellaneous (Confidential information)

Appendices 1, 2 and 3 are confidential and removed from the public thesis. The bases for secrecy are section 24(7, 17) of the Act on the Openness of Government Activities (621/1999), security arrangements of data systems and a company's business or trade secret. The period of secrecy is five (5) years, the secrecy will end on 1.11.2029.

Contents

Figures

Tables

1 Software industry, DevOps and the need for information security certification

In the software industry DevOps, Development and Operations, serves as the collaboration of development team and operations (platform) team. Lately, an added term of Security has been implemented to create DevSecOps, the part of the software development process taking care that the code and the produced products are secure for the customers and end users. Since the concept of DevSecOps is so new, first mentioned in the early 2010's (Duc, 2023), there are still a lot of things to define, best practices to create and not all companies have a clear picture what it is and how it can be utilized in their development processes.

As the demand for security gets more and more common in the cyberthreat-ridden world, software companies are wondering how to improve it in their operations. One good, even recommended, option is to rely on a framework or a standard and ISO 27001, the world's best known cyber security standard according to International Organization for Standardization (ISO) (ISO/IEC 27001, n.d.), is the most common solution. In the present thesis version ISO 27001:2023 is used.

There are many reasons for an organization to become ISO 27001 certified. In addition to wanting to operate more securely, one is that it provides existing and potential customers and collaborators reassurance that the company is doing something right regarding information and cyber security and they can be trusted with services and data. One other reason is to increase business opportunities that would otherwise be unreachable, as many companies in for example central Europe do not want to even deal with software vendors that are not certified. Without the certification business expanding plans might come to a halt, which speaks for the importance of it. Also, European Union is becoming more and more demanding concerning information security in companies, and the new NIS 2 directive coming into effect in Fall 2024 overlaps in many parts with ISO 27001.

Despite ISO 27001 being so popular and studies having been done on how to generally implement it on SMEs (e.g. Valdevit et al. 2009; Ramadhan & Rose 2022), the problem is that there are not many free or easily available guides online on how to make the actual practical improvements to a corporate environment in accordance with the standard's controls. However, lots of good advice and guidance is behind expensive consultation contracts.

The present thesis gives small to medium software businesses comprehensive guidelines how to prepare their development environment for ISO 27001 using the current best practices of the DevSecOps field. Although ISO 27001 is a standard for Information Security Management System (ISMS), and thus, it covers a large part of any company's IT and data management environment, this thesis will be limited only to parts that relate to DevOps and development infrastructure, also leaving out anything directly related to the actual code itself.

2 Research design and thesis structure

2.1 Research problem and research questions

Getting ISO 27001 certification is not a quick or easy task. It may not be obvious to a company what kind of things even affect DevSecOps, and online guides only barely scratch the surface of the topic, telling the reader to buy consultation to get more detailed help. It is true that in many cases there are not one-size-fits-all solutions. Every company's situation is different, and the amount and type of work depend heavily on the maturity of the IT and development environment. The difference in circumstances is, however, where the best practices come in, as in the end using them is what any security-minded company should aim to do. However, especially small to medium businesses are left to struggle as they often have less resources than bigger enterprises.

To help SMBs improve their security posture, the main research question of the thesis is *How to make a small to medium sized software company's DevOps compliant to ISO 27001 using industry best practices?* The thesis is divided into three parts or sub questions:

1) How to map out the current situation of DevOps regarding ISO 27001 requirements in a small-to-medium sized software company?
2) What best practices or recommendations can be found in previous research or industry-related literature about DevSecOps and compliance to any quality frameworks, especially ISO 27001?
3) How to implement ISO 27001 related DevSecOps improvements in accordance with the previously found best practices/recommendations?

2.2 Thesis structure

The thesis has seven chapters. The first is introduction to the topic and the second is describes the background of the research, like research questions, methods and the goal. Chapter three explains the theory of basic concepts needed to understand the topic.

Main work is split to three chapters based on the research questions: chapter *4 ISO 27001 and DevOps controls* contains the review on ISO 27001 standard itself to find the controls related to DevOps. Chapter *5 ISO 27001 and DevOps best practices* is the main research part where best practices for these controls are investigated and selected and chapter *6 Examples of applying ISO 27001 requirements* has practical applications for them. Lastly there is chapter *7 The outcome* for conclusions and discussion on the thesis.

2.3 Previous research and the goal of the thesis

Previous research on the exact same topic of DevSecOps and ISO 27001 is scarce. There are articles and theses on either only the development of DevSecOps and/or compliance or ISO 27001 implementations, but not all at the same time. This industry also relies heavily on peer guides, of which most can be found online using search engines for example, but the information is scattered all over smaller articles, videos and blog posts on one small topic at the time and finding a comprehensive step-by-step guide is difficult.

Thus, the goal of the thesis is to create a comprehensive step-by-step guide for small to medium sized software businesses in how to find and make the necessary DevSecOps improvements to become ISO 27001 compliant. The solution is divided into three parts based on the research sub questions: In first part the parts and controls of ISO 27001 standard related to DevSecOps are picked out and mapped to parts of the company's development infrastructure while assessing them. In the second part the industry best practices considering the ISO 27001 controls, that have been defined in part one, are examined and introduced. In the last part, concrete examples of how to make the improvements, are given.

In the big picture, the findings of the present thesis should be useful to any SME software business looking to get ISO 27001 compliant or certified. At the same time, they provide real-life concrete

examples of the improvements using Company X's environment, or a plan for needed changes that should be done later on. Also, because Company X's infrastructure is completely cloud-based, the scope of the thesis does not cover the security of on-premises equipment.

2.4 Research methods

The thesis consists of three parts. The first two are research based on literary reviews of ISO 27001 itself and various online sources found using Google search, Google Scholar and Janet Finna databases. The third part is a practical application of the best practices that have been found during the research.

In the first part, addressing the research question *how to map out the current situation of DevOps regarding ISO 27001 requirements in a small-to-medium sized software company,* ISO 27001 standard is reviewed, the parts that are related to DevSecOps are picked out, and cross-referenced to Company X's systems and documentation to get a picture of the current situation. Key personnel of the development team are given questions for information gathering purposes.

For the second part, addressing the research question *what best practices or recommendations can be found in previous research or industry-related literature about DevSecOps and compliance to any quality frameworks, especially ISO 27001*, there is a literary review on the most recent articles related to DevSecOps implementations and compliance frameworks, focusing on online resources. A literary review is necessary to gather knowledge about industry best practices and how others have implemented solutions and solved issues within this topic. The research will be narrowed down to contain only subjects that are related to the topics that have been discovered in part one.

In the third part, addressing the research question *how to implement ISO 27001 related DevSecOps improvements in accordance with the previously found best practices/recommendations*, the findings of parts one and two are cross-referenced and used to make improvements or give recommendations to improve the current situation. This last part is research-based development work, including practical implementations for Company X. The documentation for this work

is included as classified attachments to the thesis, as it contains business secrets and security solutions that cannot be publicly disclosed. However, the public version has generalized suggestions on the topics.

2.5 Background of Company X

Company X is a Finnish small-to-medium sized software company that employs around 20 people. Its main business is its own SaaS (Software as a Service) product, but they also do some development projects for different customers. There are multiple development teams that have centralized DevOps and IT infrastructure people. Currently the company is operating mainly in Finland but is looking for opportunities to expand to central Europe, especially Germany, and thus, it is planning to become ISO 27001 certified.

3 Basic concepts

3.1 Software Development

Software Development is an area of Information Technology (IT) that uses code languages to produce software of different kind to end users. There are multiple types of software, and for example IBM categorizes them as *system*, *programming*, *application* or *embedded software* (What Is Software Development?, n.d.). Software can be either open-source, that is, created by a person or a community and distributed freely, or commercial, where the software is protected, licensed and sold to the end users as a product or as a service (Difference between Open Source Software and Commercial Software, 2020).

Software development is a process. There are multiple methodologies and ways to do things, but every software project should go through the Software Development Life Cycle (SDLC): first the software needs to be planned and designed, then the code itself is implemented and it goes through testing to make sure it is viable and functions as intended (What Is Software Development?, 2023). After the code has passed the tests, it will be deployed, and the end users then get to access the software. Afterwards everything should be documented, and the process will be repeated if new features are introduced, or problems are being fixed.

There are also other aspects in doing software development, like the platform, automation tools, technologies etc., of which many are in the realm of DevOps, Development and Operations, which is explained in detail in chapter 2.2. The thesis is done from the perspective of a commercial application software producing small-to-medium business.

3.2 DevOps and DevSecOps

DevSecOps is a relatively new term and field of the IT industry. It is a shortened version of Development, Security and Operations and is used to describe the process of those three IT teams or functions working together in creating secure software (What Is DevSecOps?, n.d.-a). The basis is in DevOps, but lately the industry and software companies have become more aware of the security requirements due to the amount of cybercrime and tightening regulations, and thus have been investing in security personnel and resources to aid their development process. Traditionally, security has been almost like an afterthought and only applied at the end of the development, if at all, but DevSecOps is making security an equal part of creating software, integrated into the processes.

The purpose of DevOps is to make software development faster, easier and to produce higher quality products compared to old methods, where development team worked separately from operations and security (What Is DevOps?, n.d.). It relies heavily on automation of processes and is also a cultural change to increase collaboration between the teams. Some key concepts are containers, microservices, agile, Continuous Integration (CI) and Continuous Delivery (CD) that all improve the development process. As speed is a great factor in modern software development, and DevOps was developed also to reduce the time it takes for software to be released, adding security should not ever slow down the process, but the opposite (What Is DevSecOps?, n.d.-b). Thus, adding security to DevOps is also based on finding the correct tools, like adding Static Application Security Testing (SAST) to find problems in the code itself and Dynamic Application Security Testing (DAST) to test vulnerabilities as a penetration tester from the outside.

3.3 ISO 27001

When talking about requirements, the ISO 27001 standard has so far been the de facto IT security management framework for companies as it outlines best practices for managing information and cyber security in companies of all sizes (Kosling, 2024). It is widely known and increasingly demanded after by customers of software companies, especially bigger corporations and when making business in central Europe for example. Many companies use it as an internal framework to improve their security, but if ISO 27001 certified, a business will have something to show their clients as a proof of their compliance and commitment to security, which will be a sales advantage.

ISO 27001 is actually a standard for Information Security Management System (ISMS), which means it covers a wide range of different areas of information security in a company and focuses on giving guidelines on all the aspects that together form an ISMS. It covers all three components of people, policies, and technical implementations and follows the three principles of information security: confidentiality, integrity and availability (ISO/IEC 27001, n.d.).

The standard has an annex, that consists of controls (safeguards), that introduce recommended countermeasures to different cyber and information security risks in four groups: organizational, people, physical and technological (Martín, 2023). However, these controls are in the form of general best practices and there are no actual concrete suggestions how to implement them. This leaves it up to the companies to decide how to make the implementations, for example to decide on the use of different products or architectures, as long as they comply with the guidelines described in the controls.

ISO 27001 is widely used as a guideline only in companies for best practices in Information Security, but becoming actually certified gives the company the permission to advertise being ISO 27001 certified and the use of the ISO logo (ISO/IEC 27001, n.d.). The certification process consists of two rounds of audits by official third-party accreditors, where the ISMS and its actual implementations are verified along with, for example, on-site visits and employee interviews to make sure the policies are actually in use. The certification is valid for three years and that period includes annual audits to check that the ISMS is being taken care of even in the meantime (ISO 27001 Certification Simplified | ISMS.Online, n.d.). As the certification process becomes more expensive the more auditors have to work, a company should prepare their ISMS with great care and

have the budget for not only for internal work of putting the ISMS together, but also for these audits.

Getting ISO 27001 compliant or certified can also help with becoming compliant with for example EU regulations and directives like GDPR or NIS2. Becoming ISO 27001 certified is of course completely voluntary, though beneficial, but these regulations are not for any company operating in the EU area. For example, NIS2 directive and ISO 27001 both aim to improve cyber security in businesses, but the directive actually gives only high-level demands, like the need to have business continuity plan, but without any concrete instructions how to do that. ISO 27001 fills in with many of these kinds of demands by giving a list of actual controls to implement. However, they are not the same thing and implementing ISO 27001 does not completely fulfill the requirements for NIS2 and vice versa (Tschirpig, n.d.)Same goes for ISO 27001 and GDPR, as they also aim for different things the other being an ISMS standard and the other a directive on how to treat personal data in the EU area, but ISO 27001 can give some tools towards becoming GDPR compliant (DPM, 2021).

3.4 Compliance in software development and DevOps

According to Ramaj and colleagues (2022), when thinking about compliance in software development and DevOps, there are multiple components to consider: first, the requirements and the target state need to be known, and employees need to be made aware of them and trained. Then, when implementing, it should be done via Compliance as Code solutions and automation tools, and it is important that the use of these solutions and tools have the support of the management. Lastly, compliance should be validated by testing, continuously monitored and in the end, assessed, for example by a third-party audit or by getting an actual certification. Abrahams and Langerman (2018) list the aspects of being successful in making DevOps and DevSecOps processes compliant as competent employees, use of automated tools for both validation and testing and that the teams collaborate well.

In the present thesis compliance is looked at from the perspective of being ISO 27001 compliant on the parts that are directly related to DevOps and DevSecOps, which might include both technical controls and changes in processes or culture, while keeping in mind that the end goal is actual certification audit. ISO 27001 also offers the possibility to rule out parts that do not consider a

business for some reason and if such controls arise, there will be no practical implementation for them as the practical examples will be from the viewpoint of Company X.

4 ISO 27001 and DevOps controls

4.1 Controls related to DevOps

As mentioned in chapter 3.3 ISO 27001, ISO 27001 standard has an annex, Annex A, that is a list of best practices called controls that define what kind of actual measures the company must take in order to become compliant. The controls are divided into four groups: organizational, people, physical and technological (Martín, 2023). Organizational controls include things that the company needs to apply as organization-wide policies, like access control and different security related responsibilities. People controls list matters related to employment, for example rules regarding remote working and non-disclosure agreements. Physical controls refer to actual physical entities and their security, like who can enter the office and how the equipment there should be secured. Finally, there are technological controls, meaning the actual technology related safeguards like backups and logging.

Physical controls are out of the scope of the thesis as Company X's infrastructure is completely in the cloud, as was mentioned in chapter 2.2 The goal of the thesis, but other groups are inspected and related controls picked from them. Also, as organizational and people controls consist of company-wide policies, controls that are too high-level for the scope of the thesis have been excluded, even though they might be applicable to some parts of DevOps also.

4.1.1 Organizational controls

Organizational controls give guidelines for good management and company policies, and it is the first part of ISO 27001 Annex A. First things on the list to relate to DevOps are control 5.9, *Inventory of information and other associated assets*, where it says that "An inventory of information and other associated assets, including owners, shall be developed and maintained" along with 5.10 *Acceptable use of information and other associated assets* (ISO 27001:2023, 16). This is a good starting point, as all the assets related to the development process should be listed along with the responsible people and how to handle them properly.

Controls 5.15-5.18 discuss access control and rights, identity management and authentication processes. In technical controls there are suggestions for the actual system solutions for them, but in organizational perspective it means setting or making sure that appropriate policies are in place to protect data from unauthorized access. Referring to the asset listing mentioned above, there should be guidelines regarding who can access those assets and with what level of permissions (ISO 27001:2023, 17).

Controls 5.19-5.20 and 5.22-5.23 talk about supplier and cloud service security, so third party security is definitely one area to cover (ISO 27001:2023, 17). As Company X has all of their assets and development processes in cloud systems and it deals with subcontractors, it needs to be made sure that these third parties handle Company X and their customers' according to information security laws and best practices, there is a valid agreement between the parties and that information is not transferred to any other third parties without consent, as also required by GDPR (Irwin, 2021).

Going down the list of organizational controls, 5.28-5.29 cover service disruption situations saying that the organization should have processes for collecting evidence and maintaining information security during distress (ISO 27001:2023, 18). In practice this would mean that there should be plans for how to provide services in case of problems arising within the development infrastructure. This is especially crucial for a software company as their business depends on it.

There is some more overlapping with GDPR in controls 5.33 and 5.34, *Protection of records and Privacy and protection of personal identifiable information (PII)*. These controls define that data should be protected against "loss, destruction, falsification, unauthorized access and unauthorized release" and that data that contains information from which people can be identified, should be handled accordingly (ISO 27001:2023, 18). It should be made sure that these principles are considered during the development process.

Lastly, controls 5.36 and 5.37 mention that compliance with these rules should be reviewed regularly and that information processing guidelines should be documented (ISO 27001:2023, 18). It would be good that both of these controls were made part of the development process.

4.1.2 People controls

People controls define how to deal with the employees of the organization so that it improves information security. As mentioned in chapter 4.1 Controls related to DevOps, many of these relate to employment terms and are thus out of scope for this thesis, but there are some things that should be considered. Control 6.3 says that employees should be trained on information security rules and policies according to their role in the company, so when the organizational controls are in place, employees working in DevOps should be given education on these policies and their responsibilities related to the development environment and infrastructure (ISO 27001:2023, 19).

Remote working is acknowledged in control 6.9, saying that "security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises". As remote working is very much part of modern working culture in IT, it should be made sure that employees dealing with DevOps have a secure access to the systems and are trained to handle information securely when not in the office (ISO 27001:2023, 19).

4.1.3 Technological controls

The list of technological controls in Annex A starts with controls 8.2 and 8.3, which are about privileged access rights and information access restriction saying that "the allocation and use of privileged access rights shall be restricted and managed" (ISO 27001:2023, 20) along with same for information. They are followed by 8.4 and 8.5 defining access management for source code and development tools and how access management should be paired with secure authentication (ISO 27001:2023, 20). Combining these, it means that access to the development environment and infrastructure should be carefully thought of, planned, and implemented with the current industry best practices.

Next up are controls 8.6 *Capacity management* and 8.8 *Management of technical vulnerabilities*. Capacity management means that the capacity of resources shall be monitored and adjusted appropriately, and technical vulnerabilities management says to keep up to date with what kind of threats arise against the company's resources and infrastructure and plan mitigations. Along with control 8.9 Configuration management, which is about planning, documenting, and maintaining

configurations in the infrastructure, they are in the very core of operations part of DevOps, taking care of the systems so that services are running without disruptions (ISO 27001:2023, 21).

Controls 8.10-8.13 are once more overlapping with GDPR and define that there need to be policies and technical solutions for deleting, masking, backing up and preventing a leakage of information. Also, information processing services should be redundant enough that the information should be available according to any requirements (ISO 27001:2023, 21). In a software company loss or unavailability of customer data is a disaster, but these can also be applied to for example code.

In addition, controls 8.15 and 8.16 say that there should be logging and monitoring systems in place and that someone is actually actively following them for anomalies and problems. A minor detail is also 8.17 *Clock synchronization*, which defines that all system clocks are to be synchronized with appropriate time sources (ISO 27001:2023, 21). Nowadays most systems use common NTP (Network Time Protocol) servers, so they are in sync properly, but this is something that still needs to be checked and confirmed.

In Annex A controls 8.24-8.31 all are related to software development processes. 8.24 talks about the secure use of cryptography, 8.25-8.28 are about secure principles in coding, architecture, applications, and development life cycle, 8.29 says that there should be security testing in place, 8.30 tells to keep an eye on outsourced development and 8.31 commands to separate development, testing and production environments (ISO 27001:2023, 22). Basically, this is a chunk of controls to make developing as secure as possible.

Lastly, there are the controls of 8.32 *Change management*, 8.33 *Test information*, and 8.34 *Protection of information systems during audit testing*. These are making sure that changes to systems are planned and implemented according to that plan, that test information is chosen and used carefully and that any possible audits will not disturb the services unnecessarily (ISO 27001:2023, 22).

4.2 List of tasks based on related controls

Based on the ISO 27001 Annex A controls mentioned in chapter 4.1 *Controls related to DevOps*, a checklist of tasks has been derived and split into Table 1 *Organizational tasks*, Table 2 *People*

tasks, and Table 3 *Technological tasks*. The list consist of control name and number, target document, system or part of infrastructure and task(s) to be performed based on the control requirements. Actual suggestions for improvements and their implementations will be given in chapters 5 *ISO 27001 and DevOps best practices* and 6 *Applying ISO 27001 requirements to production*. Lifecycle in the present case means creation, changing, reviewing, maintaining, and removing of an entity mentioned in the list.

Table 1. Organizational tasks.

Control	Target	Task(s)
5.9 Inventory of information and other associated assets	Company documentation	• Make an inventory of all material and non-material assets concerning DevOps. • Define owners for each asset and assert responsible person for keeping the inventory up to date.
5.10 Acceptable use of information and other associated assets	Company documentation	• Create rules of proper handling for each asset
5.15 Access control	Company documentation	• Create a policy for accessing information
5.16 Identity management	Company documentation	• Create a policy for identity management in the company
5.17 Authentication information	Company documentation	• Create a policy for authentication information like passwords etc.

(Table 1 continues)

5.18 Access rights	Company documentation	• Create a policy for lifecycle of access rights in systems according to the access control policy
5.19 Information security in supplier relationships	Company documentation	• Make an inventory of all the suppliers regarding DevOps and risks associated with them.
5.23 Information security for use of cloud services	Company documentation	• Make an inventory of cloud services that are being used. • Create processes for cloud service life cycle from entering to exit.
5.29 Information security during disruption	Company documentation	• Create a policy for providing services during disruptions
5.34 Privacy and protection of personal identifiable information (PII)	Company documentation	• Make an inventory of all personal identifiable information that is being handled during development process or when providing services. • Create a policy for protecting this information.

Table 2. People tasks.

Control	Target	Task(s)
6.3 Information security awareness, education, and training	Company documentation, employees	• Create a policy for training development personnel in security matters related to their role. • Give out training defined in the policy and review its effectiveness.

6.7 Remote working	Company documentation, systems	• Create a policy for secure remote working for development team. • Review current processes and cross-reference with the policy. Make any changes needed.

Table 3. Technological tasks.

Control	Target	Task(s)
8.2 Privileged access rights	All systems	• Make sure that administrative rights to systems are accounted for and monitored.
8.3 Information access restriction	All systems and documentation	• Make sure that all information is behind access control and that people have access only to information required by their role.
8.4 Access to source code	Development environments	• Make sure that development environments are restricted by access control and that only necessary people can access them.
8.5 Secure authentication	All systems	• Make sure that authentication methods use best practices and are secure.
8.6 Capacity management	Platform	• Plan and implement resource monitoring and scalability so that services are not disrupted.
8.8 Management of technical vulnerabilities	All systems	• Make sure that all software in the company is accounted for and there are processes for detecting and mitigating vulnerabilities. • When developing software, create processes for vulnerability management like patching and testing.
8.9 Configuration management	All systems	• Implement a process for configuration lifecycles in all systems and services
8.10 Information deletion	All systems	• Implement a process for destruction of unneeded information.
8.12 Data leakage prevention	All systems with sensitive information	• Make sure that measures are taken against data leakage in systems that contain sensitive information

(Table 3 continues)

Table 3 (continued)

8.13 Information backup	All systems and documentation	• Create and implement a backup policy for all systems and information
8.15 Logging	All systems	• Create and implement a logging policy on all systems
8.16 Monitoring activities	All systems	• Create and implement a policy for monitoring different systems for problems and a process for handling them.
8.17 Clock synchronization	All systems	• Make sure that all systems are getting their time settings from appropriate sources
8.24 Use of cryptography	All systems	• Create and implement rules for lifecycle of cryptographic elements
8.25 Secure development life cycle	Development environments	• Create and implement policies for secure software using industry best practices
8.26 Application security requirements	Provided services	• Make sure that applications have security requirements in place.
8.27 Secure system architecture and engineering principles	Provided services	• Make sure that provided services are designed and engineered using well-known security principles.
8.28 Secure coding	Development environments	• Make sure that developers follow the principles of secure coding and industry best practices.
8.29 Security testing in development and acceptance	Development environments	• Create and implement processes for security testing in the development lifecycle.
8.30 Outsourced development	Subcontractors	• Make sure that responsibilities are defined, and an eye is kept on subcontractor activities.

(Table 3 continues)

Table 3 (continued)

8.31 Separation of development, test, and production environments	Development environments	• Make sure that development environments are separated into these different sections.
8.32 Change management	All systems	• Create and implement policies for changes in systems
8.33 Test information	Development environments	• Make sure that test information is selected and handled properly.
8.34 Protection of information systems during audit testing	Provided services	• Make sure that possible audits are planned beforehand and effects to service level are known.

4.3 Current situation in Company X

An assessment of the current situation regarding these action points has been conducted in Company X and collected into Appendix *1 Current situation in Company X* (secret). Due to the assessment including confidential information about information systems security and company trade secrets, the appendix has been made secret on the basis of section 24(7, 17) of the *Act on the Openness of Government Activities* (621/1999).

The assessment was formed by interviewing Company X's key people from their development team. The interviewees were given open questions on how they felt each control was handled in their team and answers were then combined to form a situational picture and organized into a control-by-control table to be used when planning the improvements in chapter 6.

5 ISO 27001 and DevOps best practices

After finding the controls relevant to DevOps from ISO 27001 Annex A presented in chapter 4 *ISO 27001 and DevOps controls*, implementation phase is prepared for by taking a look at best practices for each control. These recommendations below are gathered by combining different online sources and used when making the actual improvements in chapter 6 *Examples of applying ISO 27001 requirements*.

5.1 Organizational controls best practices

5.1.1 Asset protection

Control 5.9 says that there should be an inventory of information assets (ISO 27001:2023, 16). The purpose of this would be to systematically identify and protect the assets as it would be challenging to protect something the company does not know about (ISO 27001:2022 Annex A Control 5.9—What's New?, n.d.). Assets for DevOps could be for example virtual machines, development environment, source code, custom solutions, and physical storages. Basically, becoming compliant with control 5.9 requires documentation work of tangible and non-tangible assets, for which ISO 27001 does not define the presentation form, so companies are free to choose anything from Excel sheets to ISMS building software. Furthermore, the control does not define the level of detail for each asset, but for example Barker (2022) recommends at least some classification and location of the asset to be written down. As how to do the asset listing in practice, Kosutic (n.d.) suggests some good old legwork, asking around and talking to department leads about what they use in their work.

Control 5.9. also defines that the assets should have an owner and that the register should be maintained, that is, kept up to date (ISO 27001:2023, 16), so owner information should be listed along with each asset. According to Barker (2022) an asset owner is responsible for protecting, proper handling and maintaining the asset in the register and the owner can be a person or a group, but of course assigning them for a person or a role brings extra accountability.

As DevOps assets have been identified and listed after control 5.9, control 5.10 requires also acceptable use to be defined for them to protect the assets from misuse, unauthorized access, and

destruction. The company is expected to have a policy in place that covers acceptable and unacceptable use of assets and make sure that both internal and external workers are aware of the policy and consequences for noncompliance (ISO 27001:2022 Annex A Control 5.10—What's New?, n.d.). The policy should consider things like usage according to laws and requirements, ethical and unethical use, information security concerns, use for personal purposes, and means for reporting issues (5.10 Acceptable Use of Information and Other Associated Assets for ISO 27002, n.d.).

5.1.2 Managing access to systems and data

Control 5.15 tells the company to set up access control for information "*based on business and information security requirements*" (ISO 27001:2023, 17). This, again, requires a policy for accessing different systems and data. When creating a policy, a company should consider things like who needs access to said data or system, how to implement the controls and how to review the policy and access in a changing corporate environment so that it stays up to date. Good guidelines to follow would be the principles of Need to Know, Need to Use and Least Privilege, giving employees access only to things they need for performing their jobs, most commonly defined by their role. (Barker, 2023a.)

Identity management as control 5.16 means the handling of different user accounts, human and non-human, in different parts of a company's infrastructure and systems. It touches the subjects of creating them, managing their authentication and access levels, and removing them when no longer needed and the company policy should include processes and guidelines for these topics. As with access control, identities should also be regularly reviewed to ensure validity. (West, n.d.-a.) As development environments might have multiple different systems and entities accessing them, identity management protocols should be applied to prevent data and systems from rogue access.

Control 5.17 *Authentication information* defines that there should be a process for managing said information and that employees need to be trained for handling them appropriately (ISO 27001:2023, 17). In practice this means password policies: what is a secure enough password, how to deliver them to users, changing default passwords, rotating passwords regularly and consequences for misusing the passwords or when an employee goes against the policies and causes

harm. The policies can also be applied to other authentication methods, like cryptography and MFA devices. (ISO 27001:2022 Annex A Control 5.17—What's New?, n.d.)

Access rights touches the same topic as control 5.15 *Access control* but is a supplementary control to it. As control 5.15 talks about rules and policies for accessing information and assets, control 5.18 makes a point for keeping the actual technical restrictions in systems up to date, making sure that each individual's access is actually compliant to the access policy. Best practice for this would be to create a process for granting and removing access rights and how to review the rights regularly. (West, n.d.-f.)

5.1.3 Security of third parties

Control 5.19 considers relationships with suppliers and their security. As suppliers may have access to important data and systems, it is important to define the rules for them also. Essentially, supplier security comes down to creating a good policy regarding their involvement, in this thesis' case in development processes, acknowledging the risks and making sure that agreements are in place and reviewed periodically, supplier actions are monitored and supplier employees trained to comply with the rules and policies (ISO 27001:2022 Annex A Control 5.19—What's New?, n.d.). A company should also have a register of the suppliers along with their details like contact information (West, n.d.-g).

For control 5.23 a company needs to set "*processes for acquisition, use, management and exit from cloud services*" (ISO 27001:2023, 17). In practice, for acquisition this means creating policies for choosing a cloud vendor, considering for example things like compliance with security requirements and risks associated with the vendor. For use and management, the already established company policies of access control, identity management, authentication information etc. need to be applied and the cloud service monitored for risks and threats. A company needs an exit policy as well for how to transfer or delete the data and access. (Mckillop, 2024.)

5.1.4 Information security during disruption

As software companies are in many cases service providers, control 5.29 is crucial for their survival as it basically requires the company to have a business continuity and disaster recovery plans and

processes, which should also be tested regularly (Barker, 2023b). In DevOps this is especially important if a service or services are the company's main product. A good disaster recovery plan should include things like goals for restoration (Recovery Time Objective and Recovery Point Objective, how fast the recovery should be complete and how much data can be lost because of an incident), who is involved in the process, list of related assets and their details, description of backups and their processes, important contact details, and finally step-by-step guides of how to get systems running or recovered using the resources described in the plan (What Is a Disaster Recovery Plan? Definition and Related FAQs | Druva, n.d.).

5.2 People controls best practices

After defining and implementing the policies mentioned in chapter 5.2 *Organizational controls best practices*, people control 6.3 defines that the employees should be trained to be aware of and follow the policies. According to West (n.d.) it is recommended to create a training program, where employees have clear roles and responsibilities, are trained continuously and regularly and are given examples of common errors in human security or real-life security cases. The program could consist for example of awareness campaigns, emails, and information through other channels as the company seems fit. All in all, it should be encaging and regularly reviewed to ensure effectiveness. (West, n.d.-h.)

In modern software companies remote working is a routine nowadays and according to control 6.7 it should also be secured by applying security measures when people are working outside the office (ISO 27001:2023, 19). Securing remote working should include creating a policy making use of the previous policies of access rights, authentication information etc., training the users and putting related technical safeguards in place. (Barker, 2023c.) In DevOps it would be beneficial to also map out all the systems that need access through office VPN versus cloud services that are accessed over the Internet, for example.

5.3 Technical controls best practices

5.3.1 Technical access management

Privileged access rights mean that a user or an entity has access and authorization to do certain things in systems that normal users may not, quite often meaning system administrators or similar. As privileged access in the wrong hands can be very destructive, the use of it needs to be planned carefully. Some best practices would be to separate privileged (administrator) accounts from user accounts by creating separate, but personal, administrative account for those who need them, reviewing the existence of said accounts and their need regularly and to make sure that the actions of these accounts are monitored and audited. (*8.2 Privileged Access Rights for ISO 27002*, n.d.)

Control 8.3 is complementary to organizational controls of 5.15 *Access control* and 5.18 *Access rights*. There should be access control and rights policies in place, so compliance with control 8.3 means implementing the technical safeguards to follow those policies. Good practices would be centralized user management, requiring secure authentication methods, making sure that employees, third parties and anonymous users have access only to the parts of information they are meant to and that there are no information leaks. (West, n.d.-l.)

Annex A defines that "*read and write access to source code, development tools and software libraries shall be appropriately managed"* (ISO 27001:2023, 20). In practice this could be done by once again utilizing access control to code and development tools, making sure that source code is stored in a place where access control can be applied and keeping an audit trail of handling it (ISO 27001:2022 Annex A Control 8.4—What's New?, n.d.)

For control 8.5, a company should implement appropriate authentication methods for accessing any information. At least multi-factor authentication is highly recommended, but other technologies like Single Sign-On and biometric authentication can be considered (West, n.d.-i). Also, when developing software, the authentication process to the developed application needs to follow best practices, for example by applying methods against brute force attacks, making sure that authentication cannot be bypassed and passwords are never stored or transferred in plain text and keeping a log of successful and unsuccessful login attempts (Barker, 2023d).

5.3.2 Maintaining the platform

Capacity management in ISO 27001 context means that company resources should be monitored and adjusted so that business continuity will not be an issue. Resources in a software company could be virtual machines or servers and their related specifications like available memory, CPU and storage base, employees handling different roles and the amount of traffic a system, service or a database can withhold. Best ways to deal with these is to monitor business-critical services and resources for their capacity and take appropriate action when needed, making capacity plans and forecasts, and possibly applying technical solutions like automatic scaling or load balancers. (Barker, 2023e.)

For vulnerability management, a company should utilize the asset list and have a list of software at hand. There should be a vulnerability plan for the assets, which includes for example how vulnerabilities are found, how to mitigate, who is responsible for actions and what are the risks with each piece of software (Barker, 2023f). For software development this means additional measures of deciding how to find vulnerabilities, like opening a bug-bounty program or doing vulnerability scanning and penetration testing, putting patching procedures in place and keeping track of third-party libraries (ISO 27001:2022 Annex A Control 8.8—What's New?, n.d.).

Configurations can be found in systems, hardware devices, databases etc. that all should be inventoried in the asset listing. For control 8.9 compliance, a company should have processes for configuration lifecycle, meaning planning, testing, and implementing them, decide how to monitor and manage changes and have configurations backed up and test restoring them regularly. (Divya, 2023.)

If and when a company or their systems will be the target of an audit, protecting the said system during the procedures is required by control 8.34. To prevent any security issues or data leaks successfully, the audit should be planned carefully, audit procedures and scope defined beforehand, auditors should have access based on Zero Trust and Least Privilege principles, secure connections to the auditable system should be established and information security best practices like backups should be in place (West, n.d.-k).

5.3.3 Protecting information

Personal Identifiable Information (PII) means any information that a person can be identified from, for example name, contact information, date of birth etc. To comply with this control, a company should have a process for securing PII both technically and operationally *(*ISO 27001:2022 Annex A Control 5.34—What's New?, n.d.). In DevOps this means making sure that if PII is being handled as a part of providing a service for example, it is only handled by people that are required to by their role and there are technical solutions for protecting it.

Control 8.10 requires a company to delete information when it is no longer needed. To do that, a company needs to be aware of the data they collect, where it is stored and what requirements does the data have, so an information asset list will be used here. After the facts have been gathered, a policy containing deletion measures, like how it will be done and at what intervals, should be established. (Morrison, 2023.)

To take measures against data leaks, a company must first know what and where their data is and set appropriate classification and risk analysis for it and then policies for acceptable use and transfer, access control for each set of data and reporting and auditing, can be set. Technical measures include encryption, access control actions and possibly a Data Loss Prevention (DLP) system. Employees need also to be trained for correct use of data. (West, n.d.-b.)

Using the list of assets, a company should come up with backup policies for the information and systems. The policies should contain clauses for what data will be backed up and how often, where the backups will be stored, who is responsible for doing the backups and what is the restoring process, and technical issues like encryption and use of backup systems would also need to be considered. Finally, testing the backing up and restoring process regularly is necessary. (West, n.d.-c.)

Use of cryptography, most commonly encryption keys, should be planned and rules set for it. These rules should include things like what kind of data will be protected by cryptography, how and by whom the keys will be generated, how they will be securely transferred and what algorithms and protocols will be used, although the standard AES and RSA are recommended. There should also be monitoring for the use of these keys in place. (Dange, 2024.)

5.3.4 Monitoring the infrastructure

To comply with Logging control, a company should have logs of systems, network, or data access and access attempts, especially for privileged (admin) users, any changes, alerts or errors in critical systems and any attempts to shut down or bypass security controls (Doumenc, 2024). These logs should be stored securely, protected so that they cannot be tampered with or deleted, and analyzed regularly so a centralized log management with tight access control, limited privileges and preferably automated anomaly detection is recommended. Also, because in any ICT infrastructure the amount of log data is enormous, logging should be planned so that only important information from important systems is logged, and retention policies are set accordingly. (Segovia, 2015.)

Similar to control 8.15 *Logging*, actions like access and its attempts, changes and traffic in networks, systems and applications should be monitored for anomalies and threats and action taken when met with such issues (ISO 27001:2023, 21). The recommended way is to use an automated monitoring tool with alert capabilities and have a plan for how to mitigate those alerts. As with logging, because of the huge amount of information created every day in systems and network, the scope of monitoring and retention policies should also be considered. (Morrison, 2023.)

Annex A states that "*the clocks of information processing systems used by the organization shall be synchronized to approved time sources*" (ISO 27001:2023, 21). To comply, all systems should use some kind of trusted source, for example a time server, and secure network protocol for it, like NTP over Secure Socket Layer (NTPS), for their clocks. It would be good to have a backup time source and time monitoring implemented in the network and systems as well to prevent time asynchronization due to time server failure or a malicious actor. (West, n.d.-d.)

5.3.5 Secure software development

Control 8.25 requires a company to set rules for secure software development. It means that in all aspects of the development process, security should be considered starting from planning a secure architecture considering security requirements and different threat scenarios, using principles from agile development like test-driven development and peer reviews, creating proper documentation, using trusted and up-to-date development tools, third-party libraries and vulnerability scanners, and training the developers in security (Ilona, 2023).

In Annex A control 8.26 says that "*information security requirements shall be identified, specified and approved when developing or acquiring applications*" (ISO 27001:2023, 22). Simply, this means that an application should have security rules in place, and they should be followed. Things to consider would be for example authentication methods, access control, how to validate input to protect the application or system from for example injection attacks, how to protect the data from malicious actors and how to manage sessions, but depending on the application there could be other specifications as well, that should be documented and applied (Application Security with ISO 27001, n.d.).

Control 8.27 requires a company to apply the principles of secure software architecture and engineering to the systems or applications they are developing and the development process. These principles could be things like Zero Trust, Secure by Design, Defense in Depth, Least Privilege, and other well-known best practices in software architecture design. The applied principles and their practical implementations should also be documented. (ISO 27001 Annex A 8.27 Secure Systems Architecture and Engineering Principles, 2024.)

Secure coding control requests secure coding principles to be applied when developing software, for example using the principle of Code Minification and Obfuscation, avoiding shortcuts when developing, using automated tools for code reviews and scanning, monitoring third-party component security and avoiding vulnerable ones, and logging and auditing coding actions (Application Security with ISO 27001, n.d.). Control 8.29, again, is for applying security testing to the development process. The testing itself, coverage and the testing environment should be planned and set up carefully, include things like vulnerability and penetration testing, and have objectives and mitigation plans. The use of automated tools and third-party security testers should also be considered. (West, n.d.-i.)

If a company uses outsourced development or developers, their actions should be steered, monitored, and reviewed, meaning that there should be a contract between the company and the subcontractor defining rules, responsibilities, licensing etc. and having regular audits or otherwise keeping up-to-date with what they are doing (Barker, 2024.) Furthermore, control 8.31 is quite self-explanatory: for security reasons development, testing and production environments should

always be kept separate and have also separate access control and other necessary security policies (West, n.d.-e). Also, sensitive data should not exist in other environments than production (Barker, 2024b).

In Annex A control 8.32 is defined with a sentence "*changes to information processing facilities and information systems shall be subject to change management procedures*" (ISO 27001:2023, 22). A company should have change management process in place and all changes in ICT should also be submitted to it. A change management process could include things like defining the change and estimating the impact of it, deciding who is responsible for the change, how will it be carried out, how it will be communicated to employees and if training is needed, and assessing the end result of the change afterwards (Khan, 2024).

Control 8.33 sets requirements for test data to be "*appropriately selected, protected and managed"* (ISO 27001:2023, 22). Best practices would be not to use any sensitive information or at least do data masking, have similar access control to test data as for production data, preferably not use real data at all, using the data only for testing, and deleting it afterwards (Barker, 2024c).

6 Examples of applying ISO 27001 requirements

In this chapter practical implementations of the controls mentioned in previous chapters are introduced using Company X as an example. Company X uses an ISMS called Cyberday from Agendium Ltd for ISO 27001 documentation, so it will be used wherever applicable. Improvements made for Company X during this thesis will be documented in Appendix 2 *Improvements made in Company X*, which will be made secret on the same basis as Appendix 1 *Current situation in Company X,* section 24(7, 17) of the Act on the Openness of Government Activities (621/1999) due to confidential information regarding the business and ICT systems. Some controls mentioned in previous chapters have been excluded from this chapter due to the amount of workload required to comply with them being out of scope for this thesis, for example creating a whole business continuity plan, and will be touched upon in chapter 8.4 *Future research/development work*.

6.1 Asset protection

For controls 5.9 *Inventory of information and other associated assets* an asset list should be created. As mentioned in chapter 5.1.1 the exact form is not defined in the standard, so a decision should be made about in what form the list should be and where it will be stored. Also, the details of said list should be defined to suit the company but should include at least owner information for each asset.

In Cyberday control 5.9 has been divided into different tasks separated by what kind of asset is in question, for example systems, data stores and datasets, and each include information like who is responsible for the asset, how is it maintained, where is it located, how the access control is done and how is it connected to other systems or assets. An example of one asset (system) can be seen in Figure 1. *Example of a system asset*. A company can choose to use this kind of ISMS system or just make sure that the assets are listed with similar information somewhere else.

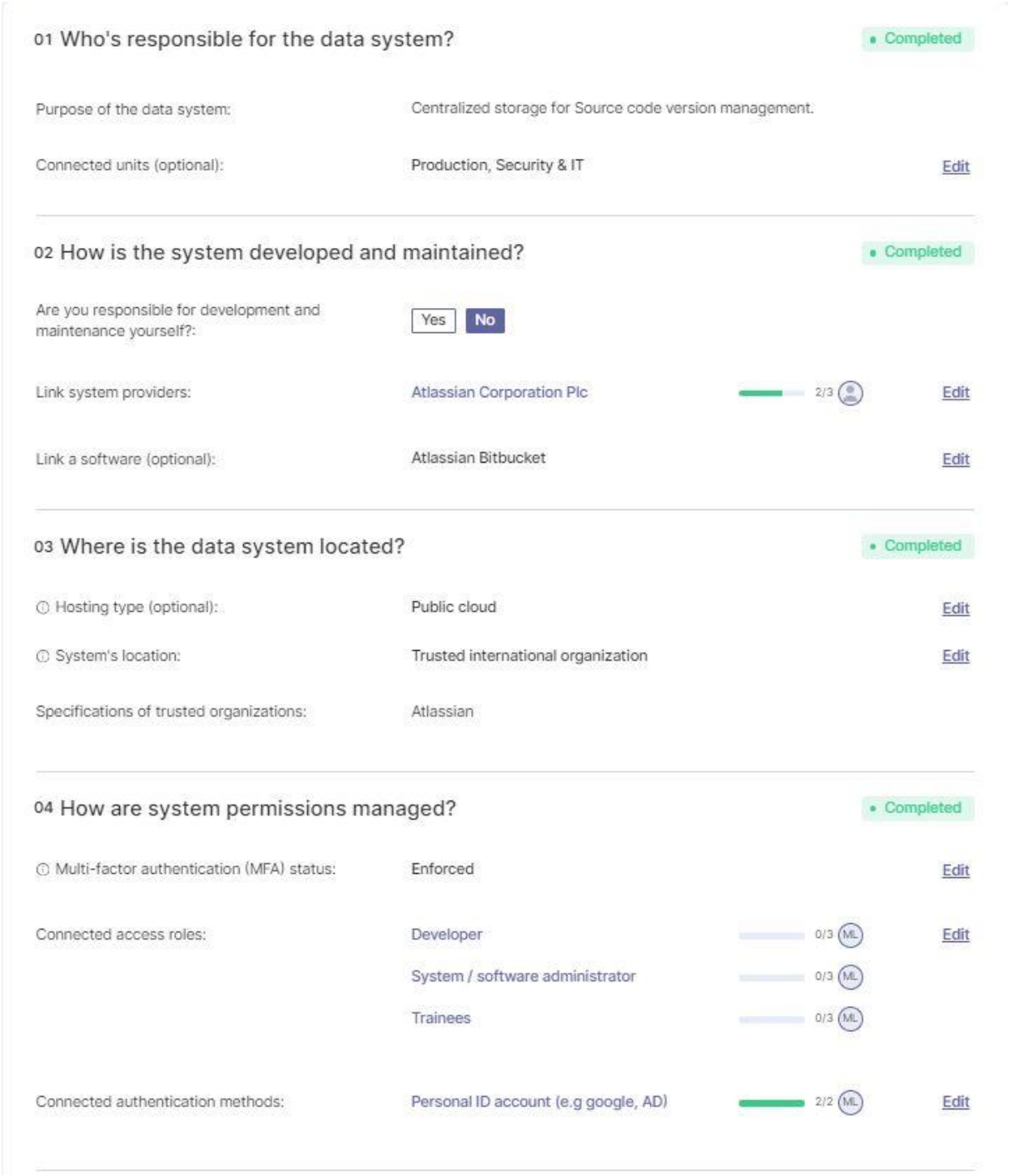

Figure 1. Example of a system asset.

A company should have a written policy available for the employees to get familiar with and sign acceptance of to avoid legal battles of responsibility in cases of neglect or abuse of information and/or systems. The policy should include at least the things listed in chapter 5.1.2 *5.10 Acceptable use of information and other associated assets* but tailored to be compliant with whatever responsibilities and regulations the company is subject to. One way to do this is include the policy in

employment contract, but it can for example be a separate document or a part of an ISMS, like in Figure 2. *Example of an acceptable use guideline* below, but as long as it is easily available to the employees and there is a register of reading and accepting it any form can do. It should also be part of the cyber security training program in the company.

In Figure 2. *Example of an acceptable use guideline* there is an example of an admin view of one guideline in Cyberday ISMS, a part of the whole policy, regarding general rules for treating personal data in data systems. As it can be seen, the rules are listed in easily readable format and there is a gauge to see how many employees out of everyone has accepted the guideline in the system. Guidelines of different topics have been combined into an acceptable use guidebook for employees to easily go through and accept them all.

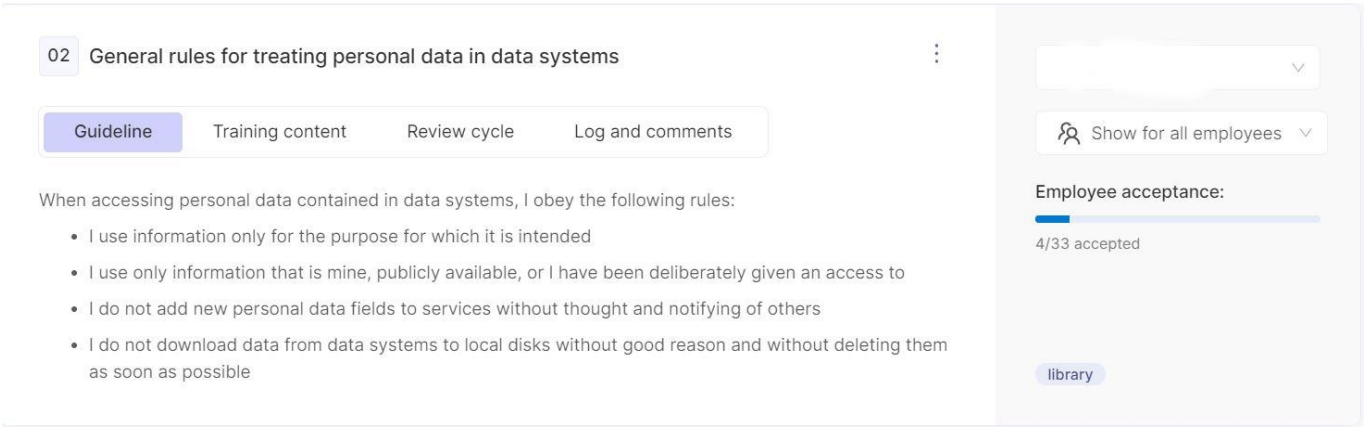

Figure 2. Example of an acceptable use guideline

6.2 Managing access to systems and data

As covered in previous chapters, managing access is a big part of ISO 27001 and the organizational part covers four controls: 5.15 Access control, 5.16 Identity management, 5.17 Authentication information and 5.18 Access rights. As all of these are closely tied together and even overlapping in some parts, it makes sense to deal with them all as one unit of access management.

Whatever policy a company chooses to use for access control considering their situation, responsibilities and legal obligations, it must be documented in written form somewhere. For example, if choosing a role-based access model, the roles should be defined and documented along with the

actual policy, which should touch topics like how access to systems or data is granted and by whom, how and when changes are done and how accessing is monitored to prevent misuse. When thinking about the policy, the access control principles a company is aiming to use should also be documented. An example of this kind of documentation can be seen in Figure 3. *Access control tasks*. below. After writing the policy down, it is also important to let the employees know about it, especially if there has been non beforehand.

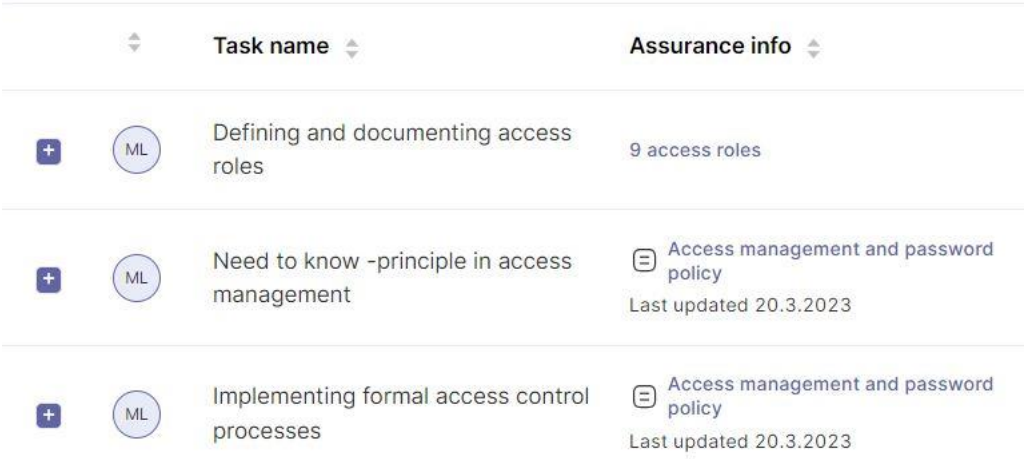

Figure 3. Access control tasks.

Identity management essentially revolves around how an individual is identified in systems to ensure accountability and a company should have a policy for this, which covers things like how they are granted access or having their access revoked, like can be seen in Figure 4. *Identity management policies.* It should also mention if identities can be shared or transferred and how those processes are handled.

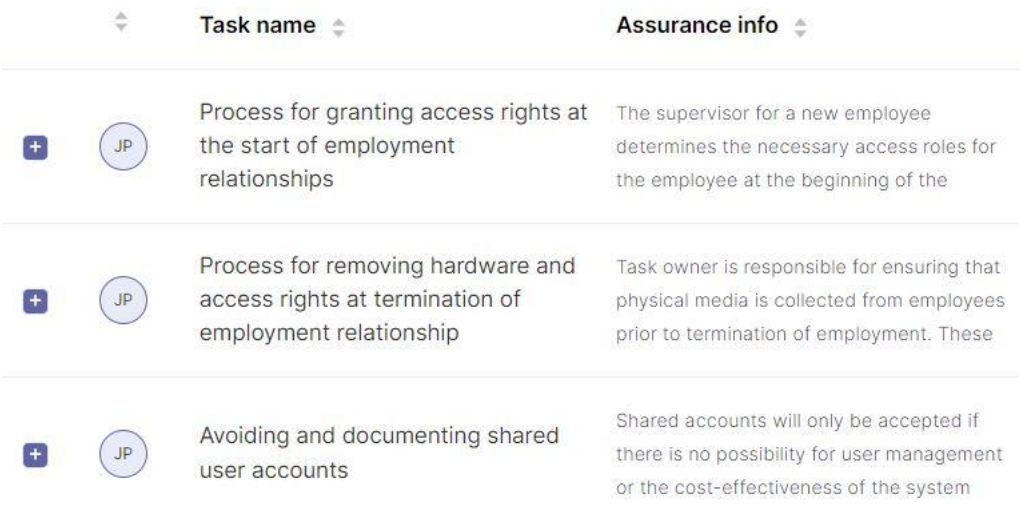

Figure 4. Identity management policies.

A policy should be written down also for authentication, including what methods to use, what is an acceptable password, if employees should use certain password manager and so on. Some examples of what kind of rules to include can be seen in Figure 5. *Authentication information policies*.

Figure 5. Authentication information policies.

Lastly in access management, policies for access rights should be defined. They are much about keeping access to systems and data up to date, so policies should include topics like how the rights are reviewed and how changes are addressed. Examples of policy topics are in Figure 6. *Examples of access rights policies*. below.

Task name
Regular reviewing of data system access rights
Instructions for reporting changes affecting access rights
Review of access right for changed employee roles
Arranging training and guidance during orientation (or before granting access rights)
Identification and management of shadow IT
Restriction of access rights at high risk times of employment

Figure 6. Examples of access rights policies.

6.3 Security of third parties

When dealing with third parties, like suppliers, partners and service providers, a set of rules and agreements should always be in place to define acceptable use of the company assets. Also, GDPR has requirements for use and privacy of third parties that need to be addressed in any privacy policy. As most companies do have these kinds of relationships with other companies, creating a policy addressing security concerns is needed.

A company should be aware of who their suppliers are, what kind of assets they have access to or what data they process, how suppliers are chosen and what should be included in the agreements. This requires creating and maintaining a supplier list and related policies. A list of example topics in a policy can be seen in Figure 7. *Examples of supplier policy topics*.

Figure 7. Examples of supplier policy topics.

A cloud service security policy should have clear rules on for example how vendors are selected, how the lifecycle (acquiring, using and exiting a service) should be handled, what kind of things are to be present in terms or description of the service, which party (provider or the customer) is responsible for which security topics, like backups or authentication methods, what kind of support is to be expected and what to do if there are incidents or vulnerabilities. Figure 8. *Examples of cloud security policy rules*. shows an example.

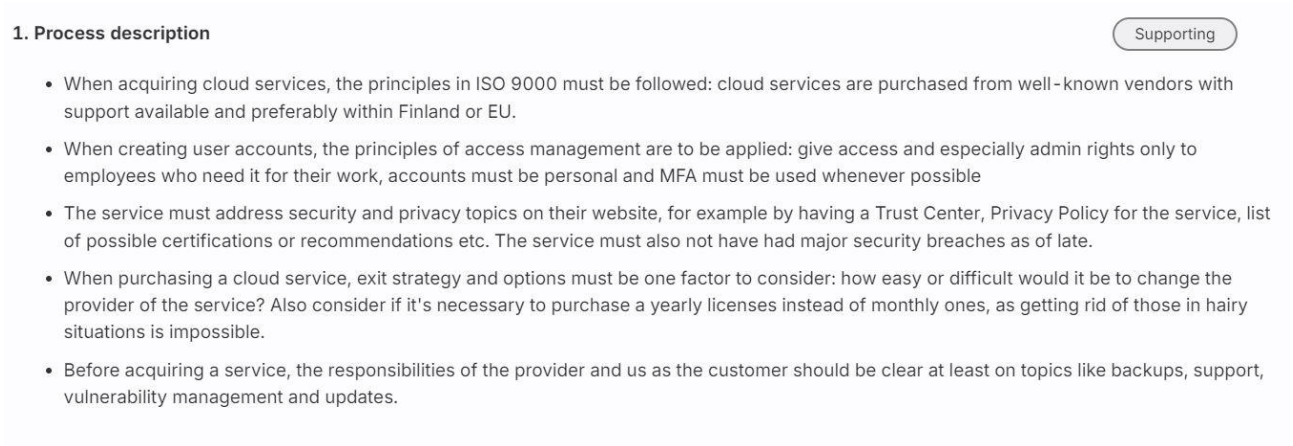

Figure 8. Examples of cloud security policy rules.

6.4 Employee related policies

Employee training might consist of for example some documentation that employees need to read and verify their understanding and willingness to comply with the rules, or regular workshops, presentations etc. that should be logged (time and who has participated), effectiveness measured by maybe some pop quizzes or questionnaires and employee feedback asked. There should also be role or department related training, as the cyber security environment and challenges are different for different employees. Combining these into a continuous or periodic training program and documenting aforementioned points will help becoming compliant with ISO 27001.

An example training program could include general and role-based information security training with signed document of receiving the training and committing to the policies when onboarding an employee, yearly renewal of such training with a final test and a signature and monthly security presentations for different departments or the whole staff about different topics along with a feedback survey at the end.

To secure remote working, the employees should have clear guidelines as to what is acceptable and what is not and how they are expected to protect their work. One obvious solution is the introduction of a VPN service, but the staff also need training, devices suited for mobile work (like laptops and mobile phones with Mobile Device Management solutions) and policies regarding for example when (following regular worktimes or working when suits them), where (is working from public places or from abroad allowed, what is required of the location) and on what they may work when remote (if there are services or data they should and can only access from the office). There is an example of general remote working policy in Figure 9. *Example of a general remote working policy.*

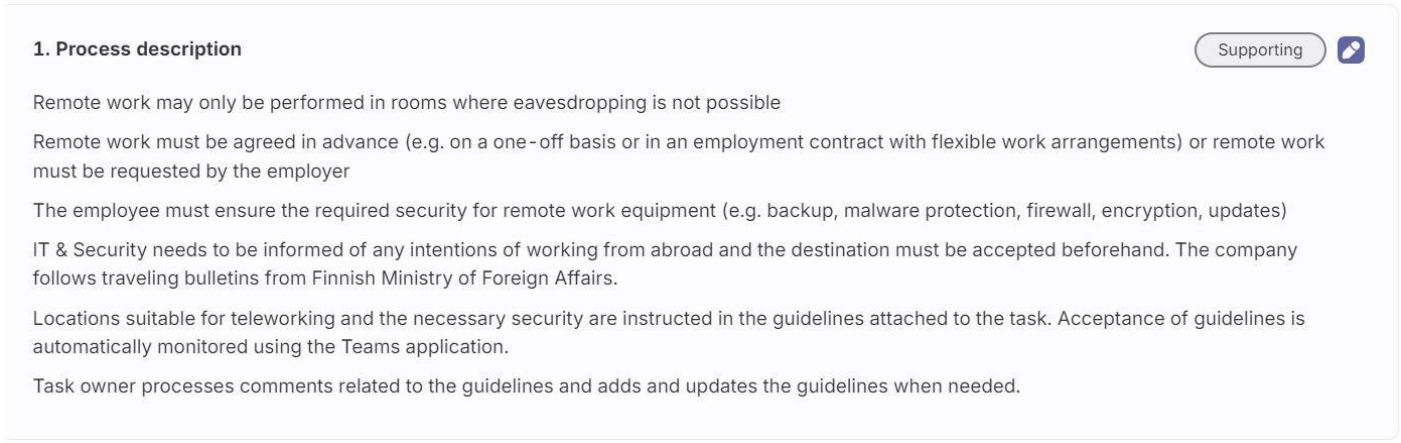

Figure 9. Example of a general remote working policy.

6.5 Technical access management

Technical access management takes the policies that have been defined in the organizational controls and applies them to systems and data by actual technical means. This requires actual handiwork and system knowledge utilizing also the asset and/or system listing done during previous steps.

First the company would need to create a policy for privileged (administrator) rights, containing rules for who can have admin access, how the permissions are granted, how they are reviewed, what kind of authentication methods are appropriate etc. An example of a privileged access policy can be seen in Figure 10. *Example of a privileged access policy*.

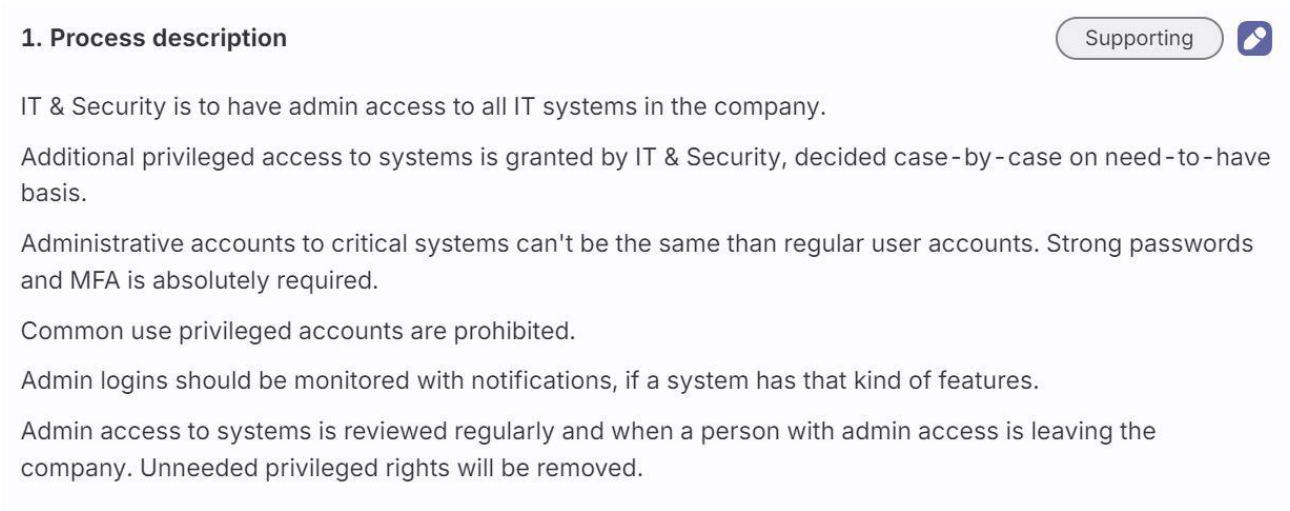

Figure 10. Example of a privileged access policy.

The best way to approach cleaning up privileged (administrator) rights is to go through them system-by-system seeing what is the current situation, revoking access from users that do not need it anymore, deciding which of the existing users need which level of permissions (if the system allows different levels), replacing general admin accounts with personal ones, seeing if all the privileged accounts are appropriately protected with passwords and MFA if possible and if it would be possible to monitor admin access and actions in the system by for example utilizing Syslog or notification features. Critical systems should be recognized, and it would be best practice to have separate administrative user accounts for those, in case of regular user account gets compromised.

Apart from systems, information also needs protecting. As discussed in previous chapters, information should be restricted to only those who actually need it to perform their job or role. Role-based access is a good policy also here, but for sensitive information even stricter access rights might be appropriate. Using the asset listing to define where data is located and applying technical access control is a good way to go about this. In addition, a company should consider taking a Data Loss Prevention (DLP) system into use to overview the use of data and notifying data security personnel of any suspicious situations.

Like other data, access to code should also be limited on need-to-know basis. In many companies code is stored in some kind of management system, like GitHub, Bitbucket etc., which have built-in access control options, like making user groups or giving repository access to people one-by-one. A

good practice is to implement role-based access here as well and create for example different groups for people who work on different projects, separate one for trainees with even more limited access and maybe there is a need for separate DevOps access as well. Wherever the code is, compliance to ISO 27001 requires that it is not openly available to everyone needlessly.

As with privileged access rights, all systems should be reviewed and checked if the authentication methods and options are following the company's authentication policy, like using centralized authentication or enforcing MFA wherever possible. Special attention should be paid to critical systems. Many systems also have other authentication options available, like logging successful and unsuccessful attempts, what kind of MFA is accepted etc., which are also worth defining.

6.6 Maintaining the platform

Whether the company has their IT platform on-premises, fully in cloud or any mix of the two, ISO 27001 has rules regarding maintaining it and preparing for problems. No matter what kind of servers a company has or where they are located, if there is anything of importance running on them, their capacity should be automatically monitored. In public cloud services there are built-in options with notification possibilities, but private cloud or on-premises servers might require buying or building a separate monitoring system, using service providers like Datadog, Zabbix etc. DevOps team should apply monitors for resource (CPU, RAM, disk capacity etc.) usage, set appropriate thresholds and make the system notify key people either directly with email, SMS or such, or alert the whole team via instant messaging services. This is especially important, if the company has SLA responsibilities or is providing critical services.

When thinking about the process for managing technical vulnerabilities in the systems the company uses or develops, they need to consider things like how vulnerabilities are discovered (what are valid information sources, if automated tools could be used, is there manual work involved etc.), what is the process for addressing and fixing the discovered vulnerabilities, how patches and updates are tested and distributed and how the process is monitored and improved whenever necessary. In Figure 11. *Example of a process addressing discovered vulnerabilities*. there is an example of a vulnerability treatment process.

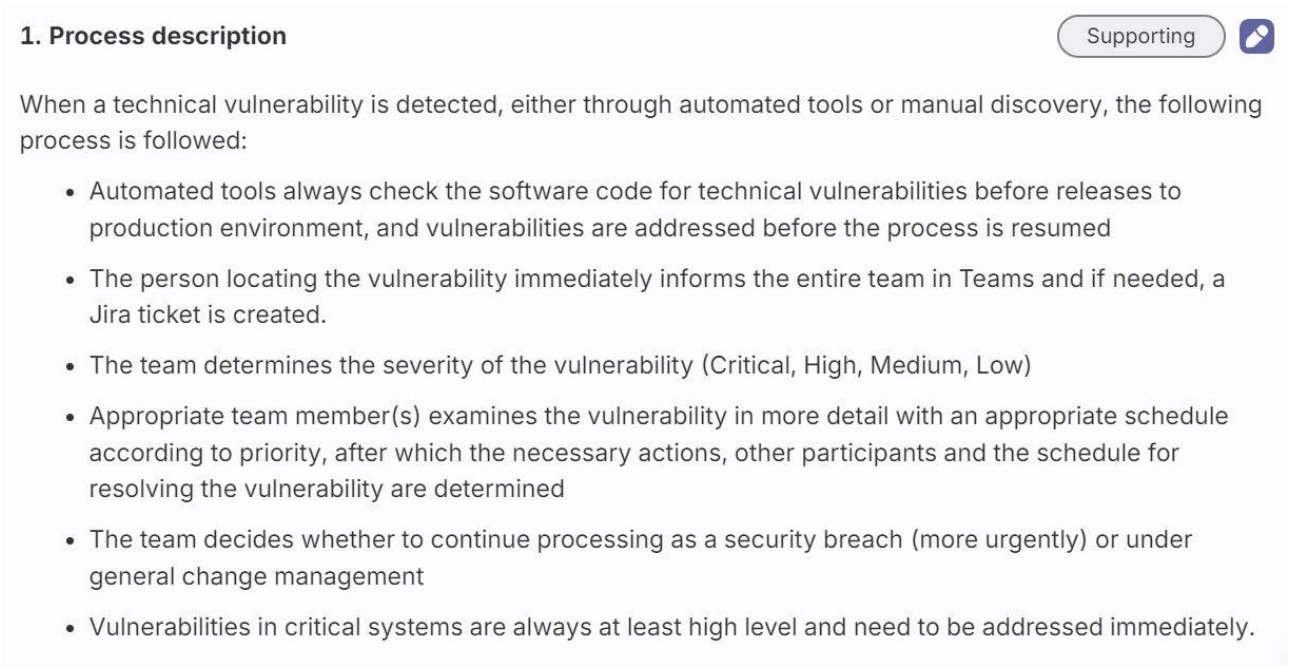

Figure 11. Example of a process addressing discovered vulnerabilities.

Additionally, in a company that develops their own software, there are also questions of how to handle issues within their own products. It is recommended to implement automatic tools for code review, vulnerability scanning and penetration testing, but the customers and/or the public should also have a channel to report any problems, as they could be a valuable asset as well. Popular scanning software are for example OWASP Zap, Burp Suite, Nessus and OpenVAS.

As configurations have the power to make or break a system, there should be processes and technical solutions to keep track of all the changes made. A good configuration policy defines who is responsible for changes, how and when they should be made, what is the testing protocol, how logging is to be done and that is the backup process. An example of a policy can be seen in Figure 12. *Example of a configuration management policy*. Also, if there is lots of repetitive configuration work, like on servers, a baseline template should be considered. Technical measures could be for example automating configuration backups, enabling changelog or audit trail and their notifications and setting up testing environments.

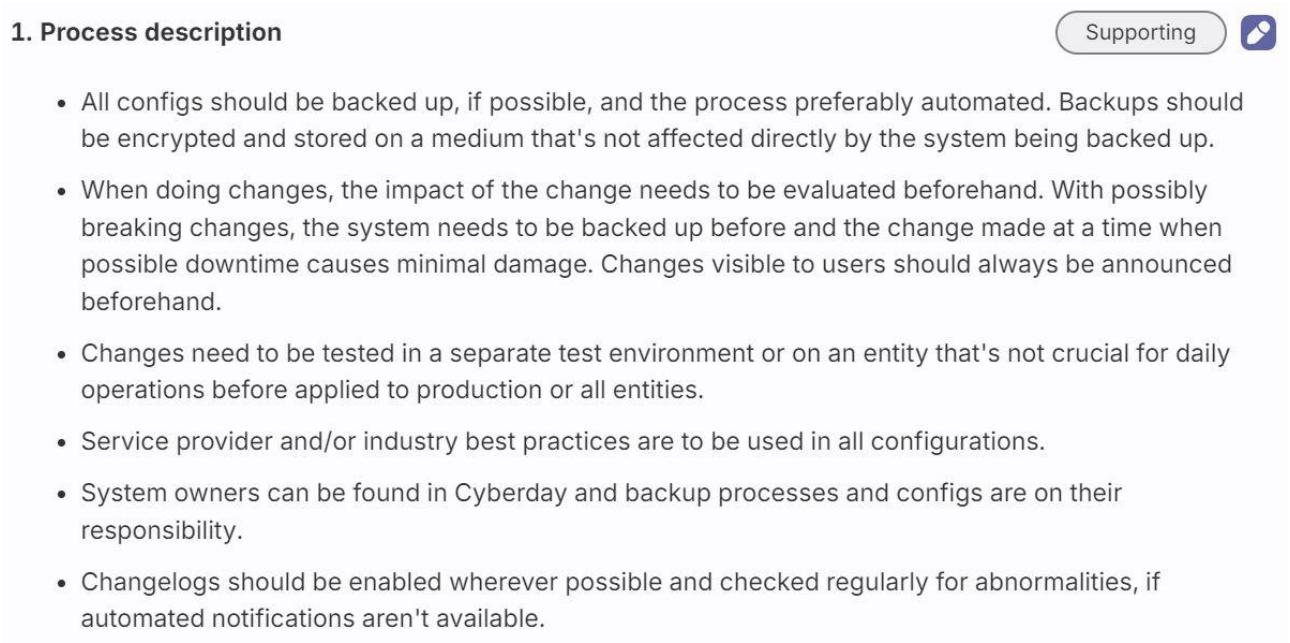

Figure 12. Example of a configuration management policy.

Sometimes companies face audits as customer requests or in order to gain a certain certification, for example. It is important to have ground rules for these situations to prevent any unplanned disruptions or damage to the systems. An example of a policy regarding audits can be seen in Figure 13. *Example of an audit policy*.

Advance planning and agreement: The organization has ensured that reviews and other verification actions targeting data systems are planned in advance and agreed upon with the appropriate testers and management. This careful planning aims to minimize the impact on operational processes.

Approval of inspection requests: The organization has established a protocol where inspection requests are approved by the appropriate responsible person, ensuring that all verification actions are authorized.

Scope agreement and monitoring: The scope of technical tests has been agreed upon in advance, and their implementation is regularly monitored. This ensures that the tests are conducted within the predefined boundaries and meet the objectives without causing unnecessary disruptions.

Read-only or experienced administration: The organization has restricted tests to read-only use as far as possible. When higher-level access is required, the tests are conducted only by experienced system administrators. This measure minimizes the risk of data corruption or unauthorized changes.

Security requirements for access devices: The organization has ensured that any devices requiring access to systems for verification actions meet the necessary security requirements in advance. This precaution helps protect the systems from potential threats.

Off-hours testing for critical systems: The organization has scheduled tests that may affect the availability of important systems to be performed outside office hours, reducing the impact on business operations.

Logging of actions and access rights: The actions taken during inspections and the access rights granted for these activities are thoroughly recorded in a log. This logging provides an audit trail and ensures accountability and transparency in the verification process.

Figure 13. Example of an audit policy.

6.7 Protecting information

In many companies the information in their systems is an irreplaceable asset and information security is a big part of ISO 27001 as well. Protecting information is also present in many legal obligations, customer contracts and industry frameworks, so giving it the attention it deserves is in the best interests of any business and should include clear policies on handling it as well as ensuring there are technical controls in place to prevent any malicious or accidental misuse.

Personal identifiable information requires special care. Policies for protecting PII can include things like appointing a Data Protection Officer (DPO) if required, keeping a list of data sets including PII, giving PII handling guidelines to employees and having procedures for data breaches and requests. List of PII protection related tasks in Cyberday can be seen in Figure 14. *List of Cyberday tasks related to PII*., which covers many of these topics. Also, in Figure 15. *Example of PII related employee guideline*. there is an example of one guideline that employees must read and agree with to be compliant with the company's information security policy.

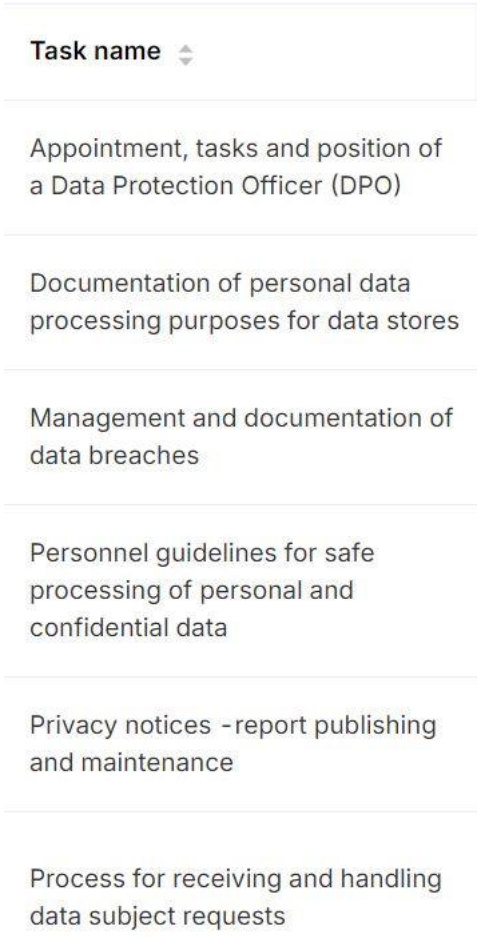

Figure 14. List of Cyberday tasks related to PII.

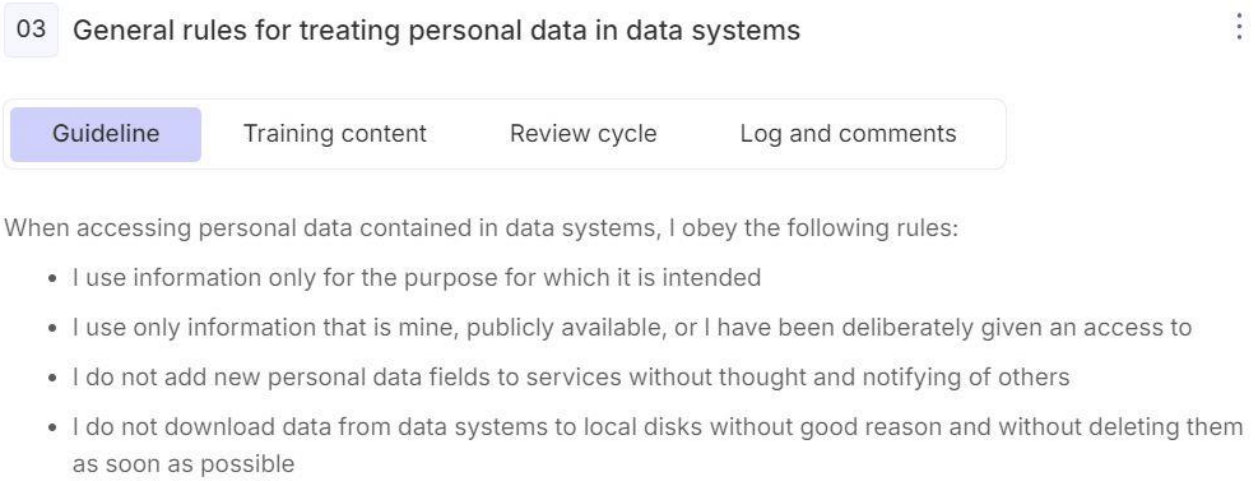

Figure 15. Example of PII related employee guideline.

Part of information security is also destroying information when it is no longer needed and doing it securely in a way that leaves evidence of deletion. All data assets should have clear rules documented on when information is deleted or if it should be archived and for how long, for example if customer data of a system is removed upon end of a contract or if it will be stored for some fixed period until final deletion. As each asset should have an owner, this would fall on their responsibility to make sure that data is handled properly at the end of its life. After GDPR storing personal information forever is no longer an option for anyone.

Factors, like how secure a deletion is needed, should also be considered and written down in data deletion policy. In cloud services data is often deleted permanently after service provider backup period is over, but on physical devices there might be a need to overwrite the drive or even destroy it physically. Whatever the method, there should be a possibility to offer some proof of deletion, as this might be asked by a customer or other data subject.

Any data leakage nowadays is not only an information security issue, but also a PR disaster and can damage the company's reputation for years to come. Thus, investing in preventing such issues is indefinitely cheaper and easier. Once information assets are recognized, they should be given different classifications depending on their confidentiality, which is a feature in many data storing services, and rules set who can handle which levels of classified information and in which systems said data should be located and where it should not be stored in any situation. A company should also make sure that data is actually stored only where the policies allow and that it is either moved or removed, if located elsewhere and that employees are trained in these rules. An actual Data Loss Prevention system (DLP) would also bring extra layer of security for information as it makes the monitoring of use of classified information automatic.

One layer of information protection is backing it up and when creating a backup strategy using for example the best practices mentioned in chapter 5.3.10 *8.13 Information backup*, it would be good to check the systems to see what kind of options they have for backups. On-premises services usually have wider possibilities than for example SaaS services, which might have none in their user interface because the service provider is doing it for their customers. Critical systems should have multiple backup mediums in different places, like a cloud version and offline, physical copies encrypted properly and stored securely.

Also to prevent data leaks and system break-ins, critical information like passwords or confidential files should always be encrypted when stored and in transit. This can be done by either encrypting the whole medium the data is on, like laptops, USB sticks etc., or encrypting just the files or data by using for example an encryption software like VeraCrypt. Operating systems like Windows and Mac OS have built-in encryption features (BitLocker and FileVault) that can be enforced on company devices to prevent information security issues if the device gets stolen or lost and they are easy to use. Also, it is highly recommended to use a trusted, company-wide password manager like Bitwarden or KeePass that encrypts the passwords as opposed to employees storing them on post-it notes or unsecure files.

When choosing encryption methods, the criticality of information should be considered. AES-256 and SHA-256 hashing algorithm are commonly used and secure, but depending on the information a company might want to use even more complex algorithms. One should also be careful where to store the encryption keys, as losing them might lead to loss of that data and implement access control on who is allowed to use the keys. Documenting policies and training employees in the use of cryptography and the risks related to unencrypted mediums and data is also needed. One example of a policy regarding encryption of portable media can be seen in *Figure 16. Example of an encryption policy*.

Figure 16. Example of an encryption policy.

6.8 Monitoring the infrastructure

There is no protecting the infrastructure from problems and threats if the personnel responsible for it are not aware of what is happening inside and on the outside of it. Administrators of the systems should set up measures to follow events, get notified about anomalies and see that there are no blind spots using for example logs and different monitoring services and dashboards.

For effective logging, systems that the company manages or develops by itself should be identified and logging details reviewed and documented, including information like what is being logged, what is the rotation period and how the logs are analyzed, and fine-tuned based on the results and company needs or requirements. One good solution is to forward all logs to a centralized log server or Security Information and Event Management (SIEM) software, that can be self-maintained or SaaS in the cloud, as long as it is separate from other systems to prevent data loss in case something happens to the original systems. For example, ElasticSearch, Graylog and Microsoft Sentinel are well-known solutions. As manual log reviewing and analyzing is not very efficient, a company should utilize automatic log analyzing and alerting tools of their chosen solution. As logs are very valuable information in problem situations or during incidents and even legally, they should also be protected properly. In Figure 17. *Example of a log protection policy*. there are some simple rules to follow.

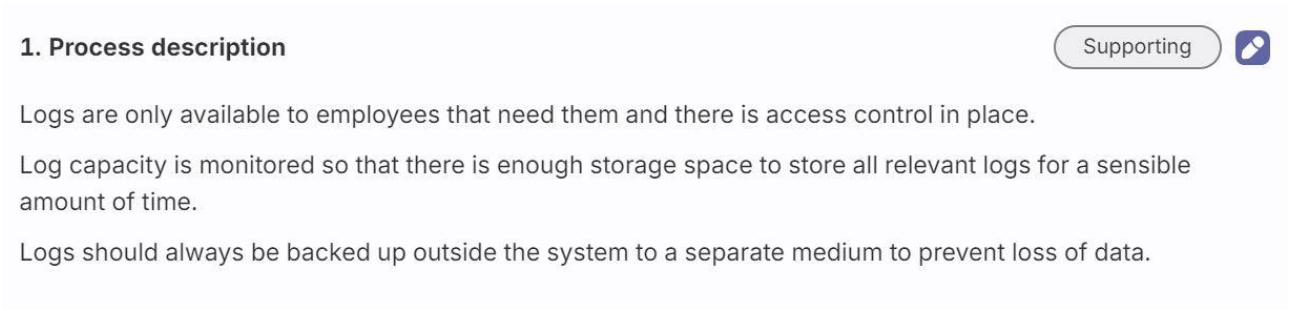

Figure 17. Example of a log protection policy.

Similar to logs, when planning a monitoring strategy, a company should identify the systems and networks they are responsible for monitoring by themselves (as opposed to a service provider) and establish a baseline for them, meaning what kind of activities are to be expected. For example, if company has no business outside Finland and there are no possibilities for remote work

from abroad, there should be no logins to systems from other countries and such attempts should be marked as anomalies. There should also be a clear flow of information documented so that employees know who to contact in case suspicious activity is detected. One example can be seen in Figure 18. *Example of communication protocol in case of anomalies*.

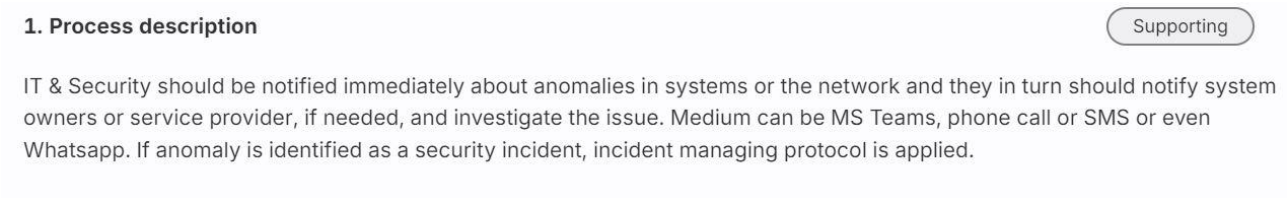

Figure 18. Example of communication protocol in case of anomalies.

Use of a centralized monitoring system is highly recommended, as it gathers all the information in one place and makes it easier for administrators to keep track of what is happening in the whole company. For example, public cloud services like MS Azure or Amazon Web Services have comprehensive built-in monitoring solutions, but there are plenty of separate, dedicated monitoring services with wide alerting capabilities, like Datadog or Zabbix.

To keep logs and monitoring accurate and easy to use, time should be synchronized across all systems by configuring them to use a trusted Network Time Protocol (NTP) source, if such configuration option is available. For example, Microsoft and Google have their own public NTP servers that anyone can use and for Linux servers there are services like ntpd and chrony that can be installed and used, instead of setting time manually.

6.9 Secure software development

In case a company is making their own software, there are additional controls and security matters to consider making the code and processes as secure as possible. This includes implementing technical systems like different code reviewing or vulnerability scanning tools, but also knowledge of secure software architectures and design. As creating a full guide on secure development is out of the scope of the thesis, the focus is on documentation work.

It would be a good practice to document the rules regarding secure development. This policy should include topics like what are the security requirements for each project, what is required of the development environment or what tools should be used, what are the skills required of the developers, how development pipeline works and what security measures are taken within it, how the integrity of the code is verified and so on. Each company should take a deep dive into their development process and write down a baseline for how everything is done and if there are any weaknesses to improve. The employee or team responsible for security in development should also be identified or named and they should be familiar with the best security practices of the industry.

Whether developing their own applications or purchasing software, a company should be aware of and document what kind of security measures are required of them, as the security of making software for military purposes differs strongly from making games, for example. The requirements can be given by for example the law, a customer or a security framework the company is using, but it should also include risk evaluation results. The criticality of the system or project can also be a factor, as a low-priority system might not need as tight security rules as a system critical to the company.

In order to implement security measures in practice, the developers should be aware of the best practices in secure architecture and development operations, which means training the developing teams in security. Security should be tightly integrated into development processes and security specialists utilized when needed. Detailed development security documentation includes the principles which are used when making system designs, be it something completely new or changes to the existing ones.

The documentation should also include clear rules for actually writing and publishing code. Good points to address are testing, reviewing and publishing processes, how possible vulnerabilities are identified and fixed, how source code is accessed and managed, how the development work (internal or using outsourced resources) is monitored and what are the definitions of done for a development task.

One important aspect of security in software development is the separation of different environments (development, testing and production) and protecting any crucial data from crossing over from production to the other two environments as it is a best practice that production data is not used in testing at all, or is used anonymized and only for a limited access and time period. Rules for using these separate environments and how test data should be protected and treated should be added to the documentation.

The last thing is to document the processes for change management, meaning how new features or improvements are planned, accepted and implemented, if the users need updates to documentation or special training, what risks are associated with the changes and what to do if the changes need to be reverted or the system needs to be restored in some other way.

7 The outcome

7.1 The conclusion of the research

The goal of the thesis was to answer the question *How to make a small to medium sized software company's DevOps compliant to ISO 27001 using industry best practices*, divided into three sub questions:

1) How to map out the current situation of DevOps regarding ISO 27001 requirements in a small-to-medium sized software company?
2) What best practices or recommendations can be found in previous research or industry-related literature about DevSecOps and compliance to any quality frameworks, especially ISO 27001?
3) How to implement ISO 27001 related DevSecOps improvements in accordance with the previously found best practices/recommendations?

Overall, the research question was answered, and the thesis forms a guide for small to medium sized software businesses in how to become compliant with or to prepare for ISO 27001 certification. The first sub question of *How to map out the current situation of DevOps regarding ISO 27001 requirements in a small-to-medium sized software company?* is addressed in chapters *4 ISO 27001 and DevOps controls* and *5 ISO 27001 and DevOps best practices* where there are lists of the things

DevOps departments should pay attention to and baselines for comparing the companies' current situation to get a picture of their starting point.

The answer to the second sub question *What best practices or recommendations can be found in previous research or industry-related literature about DevSecOps and compliance to any quality frameworks, especially ISO 27001?* is presented also in chapter *5 ISO 27001 and DevOps best practices* where a literary review is conducted on multiple online resources to find the industry recommendations for each control. Lastly, chapter *6 Examples of applying ISO 27001 requirements* offers an answer to the last question of *How to implement ISO 27001 related DevSecOps improvements in accordance with the previously found best practices/recommendations?* using Company X as an example.

7.2 Discussion on the results

While the thesis is comprehensive, it is not a complete guide to ISO 27001. Some bigger topics had to be left out due to their size making them out of scope of the thesis. On the other hand, those tasks cannot be done by DevOps department alone and require management involvement. The thesis was done by one person with help from a DevOps and developer team and thus proving that the improvements are doable by a small team in any software development company looking to improve their security posture, not just for ISO 27001 but also for NIS2 for example.

As mentioned in the introductory chapter *1 Software industry, DevOps and the need for information security certification*, there indeed were not that many different online guides in English or Finnish to give comprehensive explanations for what is required for each control and so the best practices had to be put together from small pieces of information on multiple different ISO 27001 instruction sites. Having to put together a jigsaw puzzle in that way and using so many different sources improved the trustworthiness and genericity of the recommendations. However, finding some more actual research-based articles would have added to the theory part of the thesis, as now it relies heavily on short blog posts and online articles.

What came as a surprise was the time and involvement from others that was actually required to make the improvements described in the thesis, as most software companies work in teams and typically one person cannot do all of this alone. One recommendation for companies considering

making the effort of security improvements is that they need to be sure that they actually have the time and resources to do so, as depending on their current maturity level, the changes can take months and input from multiple people and teams. One more thing that was learned during the practical part of the thesis was that anyone working on the improvements also needs to consider transition and training periods, since for example other employees and customers need to know beforehand and be trained to do things differently than before, which will delay the changes, even if the technical details would be easy and quick to implement. Management involvement and approval was emphasized many times when making the literary review and it is indeed crucial that the company really wishes to make these improvements and thinks of them as something truly valuable, as opposed to something nice to have that employees can look into whenever they have the time. Lack of management blessing and thus lack of resources will kill this kind of project very quickly as money and employee time are in that case directed in other places.

It is also a shame of how much of the practical content had to be made secret, as there would have been many helpful details there, but when dealing with topics so sensitive as cyber security, it has to be done and is understandable. The practical part also relies heavily on Cyberday ISMS that Company X uses and is thus not as generalized that maybe would be optimal, but on the other hand it is a very good example of using an ISMS and how much it can help with the work included in becoming compliant with security frameworks.

Alas, as with all technical documentation in IT, the thesis will become obsolete as technology moves forward, the ISO 27001 standard itself is updated and new best practices are defined, but for now it fulfills its goal of being a low threshold starting point of improving security in small to medium software businesses. As ISO 27001 holds many good security practices in general, the thesis is also general enough to be used as an information security improvements guide even without planning to become certified. It has also been put into bite size pieces following the controls of Annex A, making it easier to do the changes one step at a time following a logical flow.

7.3 Ethics and reliability of the research

Ethics of the research were carefully considered when planning the research and especially the documentation part, as one part of the thesis revolves around Company X's cyber security measures, politics and business secrets. Anything related to those kinds of sensitive topics were added to secret attachments, made confidential for five years and parts that were used in the public documentation, for example screenshots, were carefully checked to see that they do not accidentally reveal sensitive information. The thesis also includes data and information gathered from Company X key employees, to whom their part in the research was explained and a signed consent form was collected, and their identities covered for security purposes, as for example it would be easier to use spearhead phishing attacks when you know who are responsible for which solutions in a company. The thesis was also checked for open-source intelligence opportunities by Company X representative during client review. The plan for gathering and storing information was followed during the thesis. To increase trustworthiness, information was gathered from multiple sources that are completely external to Company X and the thesis itself. Also, the ISMS used has no other relations with Company X or their employees than being a service provider.

7.4 Future development

As mentioned in the previous chapter, the thesis is not a complete guide as some bigger topics had to be left out. One suggestion is to continue with these topics (for example the aforementioned continuity plan) from the viewpoint of a small to medium software business. Another interesting aspect of becoming compliant with frameworks or getting certification is how much effort is needed from the whole company, especially management, and not only the technical people working on the concrete improvements. It would be beneficial to look into what are the prerequisites on succeeding on this kind of project and how to prepare management and the whole staff so that the chances of going through with the project are maximized and what is actually needed from and for each team not directly related to technical aspects (like management, HR, marketing etc.) to be motivated and able to cooperate. Shortly put, the human factor in the certification process is worth further research. Future improvement suggestions for Company X are in a separate

attachment *Future improvements suggestions for Company X (secret)*, which is also made confidential on the basis of section 24(7, 17) of the Act on the Openness of Government Activities (621/1999) due to having detailed information about the company's security systems.

References

5.10 Acceptable use of Information and Other Associated Assets for ISO 27002:2022. (n.d.). Retrieved 4 June 2024, from https://www.avisoconsultancy.co.uk//iso-27001-2022-annex-a/5-10-acceptable-use-of-information-and-other-associated-assets

8.2 Privileged Access Rights for ISO 27002:2022. (n.d.). Retrieved 6 June 2024, from https://www.avisoconsultancy.co.uk//iso-27001-2022-annex-a/8-2-privileged-access-rights

Abrahams, M. Z., & Langerman, J. J. (2018). Compliance at Velocity within a DevOps Environment. *2018 Thirteenth International Conference on Digital Information Management (ICDIM)*, 94–101. https://doi.org/10.1109/ICDIM.2018.8847007

Application Security with ISO 27001. (n.d.). Retrieved 16 June 2024, from https://www.bizserveit.com/blogs/application-security-with-iso-27001

Barker, S. (2022, October 12). *ISO 27001 Annex A 5.9 Inventory Of Information And Other Associated Assets*. High Table. https://hightable.io/iso-27001-annex-a-5-9-inventory-of-information-and-other-associated-assets/

Barker, S. (2023a, January 5). *ISO 27001 Annex A 5.15 Access Control*. High Table. https://hightable.io/iso-27001-annex-a-5-15-access-control/

Barker, S. (2023b, May 6). *ISO 27001 Annex A 5.29 Information Security During Disruption*. High Table. https://hightable.io/iso-27001-annex-a-5-29-information-security-during-disruption/

Barker, S. (2023c, May 31). *ISO 27001 Annex A 6.7 Remote Working*. High Table. https://hightable.io/iso-27001-annex-a-6-7-remote-working/

Barker, S. (2023d, July 7). *ISO 27001 Annex A 8.5 Secure Authentication*. High Table. https://hightable.io/iso-27001-annex-a-8-5-secure-authentication/

Barker, S. (2023e, July 7). *ISO 27001 Annex A 8.6 Capacity Management*. High Table. https://hightable.io/iso-27001-annex-a-8-6-capacity-management/

Barker, S. (2023f, July 31). *ISO 27001 Annex A 8.8 Management of Technical Vulnerabilities*. High Table. https://hightable.io/iso-27001-annex-a-8-8-management-of-technical-vulnerabilities/

Barker, S. (2024a, January 20). *ISO 27001 Annex A 8.30 Outsourced Development*. High Table. https://hightable.io/iso27001-annex-a-8-30-outsourced-development/

Barker, S. (2024b, January 22). *ISO 27001 Annex A 8.31 Separation of Development, Test and Production Environments*. High Table. https://hightable.io/iso27001-annex-a-8-31-separation-of-development-test-and-production-environments/

Barker, S. (2024c, January 26). *ISO 27001 Annex A 8.33 Test Information*. High Table. https://hightable.io/iso27001-annex-a-8-33-test-information/

Dange, P. (2024, May 22). *ISO 27001: 2022 - Control 8.24 Use Of Cryptography*. ISO Templates and Documents Download. https://iso-docs.com/blogs/iso-27001-2022-standard/iso-27001-2022-control-8-24-use-of-cryptography

Difference between Open source Software and Commercial Software. (2020, October 10). GeeksforGeeks. https://www.geeksforgeeks.org/difference-between-open-source-software-and-commercial-software/

Divya. (2023, October 9). Understanding ISO 27002:2022 Control 8.9. *SIS Certifications*. https://www.siscertifications.com/understanding-iso-27002-2022-control-8-9/

Doumenc, F. (2024, February 9). *What are the ISO 27001 Logging Requirement ?* https://trout.software/blog/iso-27001-logging-and-monitoring

DPM. (2021, August 4). *What is the Difference Between GDPR and ISO 27001*. Data Privacy Manager. https://dataprivacymanager.net/what-is-the-difference-between-gdpr-and-iso-27001/

Duc, H. N. (2023, July 5). *History of DevSecOps—eForensics*. https://eforensicsmag.com/history-of-devsecops/

Ilona. (2023, September 20). Turvallinen ohjelmointi – uusi ISO 27001:n hallintakeino. *2ns*. https://www.2ns.fi/turvallinen-ohjelmointi-uusi-iso-27001n-hallintakeino/

Irwin, L. (2021, July 26). *Data Sharing Agreements and GDPR: What You Need To Know*. GRCI Law Blog. https://www.grcilaw.com/blog/what-you-need-to-know-when-drafting-data-sharing-agreements

ISO 27001 Annex A 8.27 Secure Systems Architecture and Engineering Principles. (2024, January 12). High Table. https://hightable.io/iso27001-annex-a-8-27-secure-systems-architecture-and-engineering-principles/

ISO 27001 Certification Simplified | ISMS.online. (n.d.). Https://Www.Isms.Online/. Retrieved 17 May 2024, from https://www.isms.online/iso-27001/certification/

ISO 27001:2022 Annex A Control 5.9—What's New? | ISMS.online. (n.d.-a). Https://Www.Isms.Online/. Retrieved 4 June 2024, from https://www.isms.online/iso-27001/annex-a/5-9-inventory-of-information-other-associated-assets-2022/

ISO 27001:2022 Annex A Control 5.10—What's New? | ISMS.online. (n.d.-b). Https://Www.Isms.Online/. Retrieved 4 June 2024, from https://www.isms.online/iso-27001/annex-a/5-10-acceptable-use-of-information-other-associated-assets-2022/

ISO 27001:2022 Annex A Control 5.17—What's New? | ISMS.online. (n.d.-c). Https://Www.Isms.Online/. Retrieved 4 June 2024, from https://www.isms.online/iso-27001/annex-a/5-17-authentication-information-2022/

ISO 27001:2022 Annex A Control 5.19—What's New? | ISMS.online. (n.d.-d). Https://Www.Isms.Online/. Retrieved 6 June 2024, from https://www.isms.online/iso-27001/annex-a/5-19-information-security-supplier-relationships-2022/

ISO 27001:2022 Annex A Control 5.34—What's New? | ISMS.online. (n.d.-e). Https://Www.Isms.Online/. Retrieved 6 June 2024, from https://www.isms.online/iso-27001/annex-a/5-34-privacy-and-protection-of-pii-2022/

ISO 27001:2022 Annex A Control 8.4—What's New? | ISMS.online. (n.d.-f). Https://Www.Isms.Online/. Retrieved 11 June 2024, from https://www.isms.online/iso-27001/annex-a/8-4-access-to-source-code-2022/

ISO 27001:2022 Annex A Control 8.8—What's New? | ISMS.online. (n.d.-g). Https://Www.Isms.Online/. Retrieved 11 June 2024, from https://www.isms.online/iso-27001/annex-a/8-8-management-of-technical-vulnerabilities-2022/

ISO/IEC 27001:2022. (n.d.). ISO. Retrieved 18 April 2024, from https://www.iso.org/standard/27001

Khan, A. (2024, May 20). *ISO 27001:2022-Controls 8.32-Change Management*. ISO Templates and Documents Download. https://iso-docs.com/blogs/iso-27001-2022-standard/iso-27001-2022-controls-8-32-change-management

Kosling, K. (2024, March 27). *5 Benefits of ISO 27001 Certification*. IT Governance Blog En. https://www.itgovernance.eu/blog/en/benefits-of-iso-27001-certification

Kosutic, D. (n.d.). *ISO 27001 Asset Management: Develop an ISO 27001 asset register*. Retrieved 4 June 2024, from https://advisera.com/27001academy/knowledgebase/how-to-handle-asset-register-asset-inventory-according-to-iso-27001/

Martín, D. (2023, July 24). ISO 27001: What are the main controls of this standard? *GlobalSuite Solutions*. https://www.globalsuitesolutions.com/iso-27001-what-are-the-main-controls-of-this-standard/

Mckillop, C. (2024, April 18). *MSP ISO 27001:2022 A.5.23: Ensuring Cloud Services Security for Managed Service Providers—GRC For MSPs: Your Trusted GRC Sidekick for ISO 27001 Certification*. https://grcformsps.com.au/2024/04/18/msp-iso-270012022-a-5-23-information-security-for-use-of-cloud-services/

Morrison, D. (2023a, July 20). *ISO 27001:2022—8.10 Information deletion—Morrisec*. https://morrisec.com.au/iso-27001-2022-8-10-information-deletion/

Morrison, D. (2023b, September 7). *ISO 27001:2022—8.16 Monitoring Activities—Morrisec*. https://morrisec.com.au/iso-27001-2022-8-16-monitoring-activities/

Ramaj, X., Sánchez-Gordón, M., Gkioulos, V., Chockalingam, S., & Colomo-Palacios, R. (2022). Holding on to Compliance While Adopting DevSecOps: An SLR. *Electronics*, *11*(22), 3707. https://doi.org/10.3390/electronics11223707

Segovia, A. J. (2015, November 23). *ISO 27001 logging: How to comply with A.8.15*. https://advis-era.com/27001academy/logging-according-to-iso-27001/

Tschirpig, C. (n.d.). *(Blog) ISO 27001 and NIS2: Understanding their Connection | Academy | Cyberday.ai*. Retrieved 20 May 2024, from https://www.cyberday.ai/blog/iso-27001-and-nis2-connection

West, H. (n.d.-a). *How to Implement ISO 27001 Annex A 5.16 [+ Examples]*. Retrieved 4 June 2024, from https://www.grcmana.io/blog/iso-27001-annex-a-5-16

West, H. (n.d.-b). *How to Implement ISO 27001 Annex A 8.12 [+ Examples]*. Retrieved 11 June 2024, from https://www.grcmana.io/blog/iso-27001-annex-a-8-12

West, H. (n.d.-c). *How to Implement ISO 27001 Annex A 8.13 and Pass Your Audit*. Retrieved 11 June 2024, from https://www.grcmana.io/blog/iso-27001-annex-a-8-13

West, H. (n.d.-d). *How to Implement ISO 27001 Annex A 8.17 and Pass Your Audit*. Retrieved 16 June 2024, from https://www.grcmana.io/blog/iso-27001-annex-a-8-17

West, H. (n.d.-e). *How to Implement ISO 27001 Annex A 8.31 [+ Examples]*. Retrieved 16 June 2024, from https://www.grcmana.io/blog/iso-27001-annex-a-8-31

West, H. (n.d.-f). *ISO 27001 Annex A 5.18: The Ultimate Certification Guide*. Retrieved 4 June 2024, from https://www.grcmana.io/blog/iso-27001-annex-a-5-18

West, H. (n.d.-g). *ISO 27001 Annex A 5.19: The Ultimate Certification Guide*. Retrieved 6 June 2024, from https://www.grcmana.io/blog/iso-27001-annex-a-5-19

West, H. (n.d.-h). *ISO 27001 Annex A 6.3: A Step-by-Step Guide*. Retrieved 6 June 2024, from https://www.grcmana.io/blog/iso-27001-annex-a-6-3

West, H. (n.d.-i). *ISO 27001 Annex A 8.5: A Step-by-Step Guide*. Retrieved 11 June 2024, from https://www.grcmana.io/blog/iso-27001-annex-a-8-5

West, H. (n.d.-j). *ISO 27001 Annex A 8.29: A Comprehensive Guide*. Retrieved 16 June 2024, from https://www.grcmana.io/blog/iso-27001-annex-a-8-29

West, H. (n.d.-k). *ISO 27001 Annex A 8.34: The Ultimate Guide*. Retrieved 16 June 2024, from https://www.grcmana.io/blog/iso-27001-annex-a-8-34

West, H. (n.d.-l). *ISO27001 Annex A 8.3: A Comprehensive Guide*. Retrieved 6 June 2024, from https://www.grcmana.io/blog/iso-27001-annex-a-8-3

What is a Disaster Recovery Plan? Definition and Related FAQs | Druva. (n.d.). Retrieved 20 November 2022, from https://www.druva.com/glossary/what-is-a-disaster-recovery-plan-definition-and-related-faqs/

What is DevOps? (n.d.). Retrieved 18 April 2024, from https://about.gitlab.com/topics/devops/

What is DevSecOps? (n.d.-a). Retrieved 18 April 2024, from https://www.redhat.com/en/topics/devops/what-is-devsecops

What is DevSecOps? - Developer Security Operations Explained - AWS. (n.d.-b). Amazon Web Services, Inc. Retrieved 18 April 2024, from https://aws.amazon.com/what-is/devsecops/

What is Software Development? (2023, November 1). GeeksforGeeks. https://www.geeksforgeeks.org/what-is-software-development/

What Is Software Development? | IBM. (n.d.). Retrieved 18 April 2024, from https://www.ibm.com/topics/software-development

Appendices

Appendix 1. Current situation in Company X (secret)

Appendix 2. Improvements made in Company X (secret)

Appendix 3. Future improvements suggestions for Company X (secret)