Design, Implementation, and Evaluation of ISO 27001 Process Controls in IT Infrastructure: An Analysis of Risk Probability and Process Efficiency

University of Turku
Department of Computing
Master of Science (Tech) Thesis
Cybersecurity Technology
March 2026
Joonas Salminen

Supervisors:
Petri Sainio
Naz Nebile Karataş

UNIVERSITY OF TURKU
Department of Computing

JOONAS SALMINEN: Design, Implementation, and Evaluation of ISO 27001 Process Controls in IT Infrastructure:
An Analysis of Risk Probability and Process Efficiency

Master of Science (Tech) Thesis, 65 p.
Cybersecurity Technology
March 2026

ISO/IEC 27001:2022 is a cybersecurity standard developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), against which organizations can certify their Information Security Management System (ISMS). This thesis has been carried out with an organization operating in the IT industry. ISO/IEC 27001 is a widely recognized standard, and the organization has therefore chosen to certify its ISMS against it. The increasing number of cyber threats, growing regulatory requirements, and customer expectations serve as the primary drivers for pursuing certification.

A literature review is conducted to establish a foundational understanding of the subject and to examine the requirements of the standard. The empirical part of the research is carried out as a case study for the organization. Six controls from Annex A of ISO/IEC 27001 are selected for design and implementation in order to strengthen the cybersecurity of the organization's IT infrastructure and ensure compliance with the standard.

A qualitative analysis is performed to assess how the implemented controls mitigate identified risks, how they influence process efficiency, and whether opportunities exist for automation to reduce any negative impacts on efficiency. The findings indicate that the implemented controls are effective in mitigating threats. However, the increased need for documentation reduces process efficiency. Consequently, several automation opportunities are proposed to minimize these negative effects.

Keywords: ISO/IEC 27001, cybersecurity, IT infrastructure, Information Security Management System, Annex A controls

Contents

1 Introduction

This thesis has been carried out with an IT company (hereafter referred to as the target organization) operating primarily in software development. The target organization provides solutions in software architecture and development, data and integration, artificial intelligence, cybersecurity, and maintenance and support. Its main focus is in the industrial sector, with customers also in, for example, the financial and public sectors. This introduction presents the background and motivation for the thesis, the problem it aims to address, the main objective, the research questions, the scope and limitations, research methodology, and the overall structure of the thesis.

1.1 Background and Motivation

The role of information security is constantly increasing. Organizations rely more extensively on digital services to support their core business functions. As a result, they must adopt robust security strategies to safeguard their assets. A well-established security infrastructure also enables organizations to comply with various standards and regulatory requirements. [1] The ISO/IEC 27001:2022 standard (hereafter referred to as ISO 27001 standard) is ISO's most widely adopted information security standard. This is because organizations receive great benefits from implementing their Information Security Management System (ISMS) in accordance with it. [2] Among other reasons, the standard is also applicable across all business sectors [2,

3]. Therefore, the target organization has chosen to certify its ISMS against ISO 27001 standard.

The ISO Survey tracks the number of ISO certificates granted worldwide. Based on several sources that have examined ISO Survey results across different years, it is evident that the number of ISO 27001 certificates is steadily increasing. Although the exact number of certified organizations is not publicly available, the survey provides a reasonable estimate. According to the survey, there were 31,910 certified organizations in 2018. By 2021, this number had risen to 58,687, and in 2024 the number had reached 96,709. [4–9]

Customer interest in certification is also increasing. For example, Etteplan notes in a blog post that customer expectations strongly influenced their decision to seek certification [10]. Already in 2016, 71% of respondents to the ISO Survey reported being asked whether they held an ISO 27001 certificate [11]. Given the significant growth in certified organizations since then, it is reasonable to assume that demand has continued to rise.

Some customers of the target organization have likewise begun requesting, or even requiring, ISO 27001 certification as part of competitive tendering. As with many other organizations, the primary motivations for the target organization to pursue the certification are to improve its information security practices and enhance its competitiveness in bidding processes [12]. Certification demonstrates to potential customers that the target organization takes information security seriously and that its security measures have been independently audited.

1.2 Problem Statement

The problem is that the target organization lacks a sufficiently comprehensive ISMS to achieve ISO 27001 certification. Although some controls are already in place, they are not adequate from the perspective of the standard. There is a clear gap between

the current and desired state. This gap will later be analyzed from the perspective of selected controls. Additionally, the target organization does not know how the controls will affect the efficiency of the processes within scope. Therefore, a systematic approach to designing and implementing the controls, as well as evaluating their impact, is essential to ensure both compliance and operational efficiency.

1.3 Objective of the Thesis

The objective of this thesis is to identify appropriate solutions for the needs of the target organization. Every organization has unique infrastructure and business requirements. Although the controls listed in Annex A of the ISO 27001 standard's documentation outline what should be addressed, the specific measures must always be tailored to the organization's context. The objective is to design and implement controls for the target organization's IT infrastructure-related processes in a way that supports compliance with ISO 27001 standard's requirements.

Another objective is to analyze the impact of the implemented controls on the risks they are intended to mitigate. From a resource-efficiency perspective, it is important that the controls do not introduce excessive additional workload. The goal of implementing the controls is not to increase bureaucracy, but to enhance security. Therefore, this thesis evaluates the efficiency of the relevant processes and seeks solutions that ensure compliance with the ISO 27001 standard without significantly reducing performance.

A third objective is to examine whether opportunities exist to automate the processes, or parts of them. This includes investigating whether automation could reduce negative effects or even improve efficiency compared to the situation prior to implementation. Automation should aim to minimize repetitive manual tasks. The goal is to identify tasks that are currently performed manually but could be automated to reduce the time required to execute control-related activities. All

research questions are answered in Chapter 5.

1.4 Research Questions

This thesis addresses the following three research questions:

RQ1: How do the implemented process controls in IT infrastructure affect the probability of the risks they are designed to mitigate?

RQ2: What is the impact of these controls on process efficiency?

RQ3: Can automation reduce negative effects or enhance the efficiency of the processes?

1.5 Research Methodology

The research methodology of this thesis consists of two main components: a literature review and an empirical case study. The literature review serves as a basic research and includes an examination of academic publications, standard documentation, and design and implementation guides related to selected ISO 27001 standard's controls. Its purpose is to establish a theoretical foundation for designing the chosen controls. The second component, the empirical research, is conducted as an applied case study within the target organization. This approach is appropriate because the aim is not only to design the controls but also to implement them in practice. The case study enables an examination of how the implemented controls influence risks and process efficiency, as well as whether certain parts could be automated for improved results.

A qualitative analysis is applied in the evaluation phase. This method has been chosen because collecting reliable quantitative metrics on risks and efficiency within the limited timeframe of the thesis is challenging. Qualitative data consists of ob-

servations and documentation analysis, which are used to assess the effects of the implemented controls and to evaluate automation possibilities.

1.6 Scope and Limitations

The scope of this thesis is limited to ISO 27001 standard's Annex A controls that relate to IT-infrastructure-related processes of the target organization. This scope was chosen to restrict the number of controls that must be examined, allowing the thesis to cover the entire lifecycle of selected controls from start to finish. This includes gap analysis, design, implementation, evaluation of risk mitigation, and assessment of impacts on process efficiency.

There are also limitations affecting this thesis. Due to the sensitivity of certain information, not all details can be disclosed. Detailed descriptions of the target organization's IT infrastructure, identified risks, and vulnerabilities have been omitted or discussed only at a general level. These limitations are necessary for operational security with the purpose of protecting the target organization's critical assets. Although this restricts the level of detail that can be presented, it is still possible to describe the processes and findings sufficiently to provide a clear overall picture and address the research questions.

1.7 Structure of the Thesis

The remainder of the thesis is structured as follows. Chapter 2 establishes a basic understanding of the ISO 27001 standard and the certification process. Relevant controls are also introduced. Risk management in IT infrastructure and key implementation considerations are discussed. Chapter 3 presents the current situation of the target organization, examining existing risks, vulnerabilities, and limitations of current processes. Chapter 4 focuses on the empirical part of the thesis, describing

the design considerations and implementations of the controls. Chapter 5 analyzes the effects of the controls on risks and process efficiency, and explores possibilities for automation. All research questions are addressed in Chapter 5. Chapter 6 concludes the thesis.

1.8 Declaration of the Use of Artificial Intelligence

While writing this thesis, Microsoft Copilot was used solely for grammar checking and for rephrasing sentences to produce more idiomatic English. All content was created by the author of this thesis, and AI was used only to enhance the linguistic quality of the text.

2 ISO 27001 Standard and the Role of Process Controls in Information Security

In this chapter, a basic understanding of the Information Security Management System (ISMS) and the ISO 27001 standard is established. These topics must be reviewed to understand why and how the requirements of the standard should be met. The chapter also examines how security is managed within IT infrastructure. Moreover, it introduces the six controls that are ultimately designed and implemented in practice to help the target organization comply with ISO 27001 requirements and strengthen the security of its IT infrastructure. Finally, considerations for implementing controls in both on-premises and cloud environments are briefly discussed at the end of this chapter.

2.1 Information Security Management System (ISMS)

To understand the ISO 27001 standard and its controls, it is essential to understand what an ISMS is. An ISMS is necessary for organizations to ensure continuity of business operations in the event of an information security incident [13, 14]. The primary goal of an ISMS is to strengthen information security in order to support the achievement of business objectives [15]. Its purpose is to preserve the confidentiality,

integrity, and availability of information [3, 13, 14, 16–18].

Alavi et al. [13] define an ISMS as creating the foundation for a security framework and providing a systematic approach for information systems to securely use available information. They also add authenticity and auditability to the core objectives of confidentiality, integrity, and availability. Alrehili and Alhazmi [17] describe an ISMS as "a series of structured processes that systematically create, document, and continually manage procedures aimed at enhancing the security and dependability of an organization's assets".

Policies, procedures, guidelines, and related resources and activities form an essential part of an ISMS [15, 19]. Policy documents represent the organization's high-level target state and are approved by top management [14, 15]. More detailed procedural documents may be created based on these policy documents [20]. These documents provide step-by-step guidance on how the policies are implemented in practice [14]. Thus, an ISMS is not just a collection of technical measures used for protecting the organization's information assets. It must also incorporate non-technical elements [13, 14].

With a well-established ISMS, organizations can effectively implement the necessary controls to mitigate risks [14, 15]. According to ISOfocus [21], an ISMS based on the ISO 27001 standard is "one of the most effective risk management tools for fighting off the billions of attacks that occur each year". An ISMS is developed based on a risk assessment and the organization's risk acceptance criteria [15].

An ISMS is successfully implemented when appropriate controls are established to protect critical information assets. Several key factors are required for successful implementation. [15] First, everyone in the organization must understand the importance of information security [13, 15]. This includes management and stakeholders [3, 13, 15–18]. It is also essential to establish clear roles and responsibilities for various information security functions [3, 13, 15–17]. Furthermore, the ISMS

should align with the organization's values to encourage everyone to follow it [15]. Risks must be assessed to determine which controls are needed to reduce them to an acceptable level [14, 15]. Security should be integrated into networks and systems by design. Potential incidents should be proactively prevented and detected, and information security must be managed comprehensively [15]. Finally, the ISMS should be continuously evaluated, and necessary improvements should be made [15, 18].

In today's environment, having an ISMS is almost a necessity. Implementing an ISMS should be a strategic decision made by the organization [15, 16, 19]. It should meet the organization's needs and be seamlessly integrated into its security culture [15, 22]. Risks must be managed to reduce their impact on organization's business functions, and the ISMS is designed precisely for this purpose [14, 15]. Successful implementation of an ISMS ensures that organization's information assets are protected, enabling the organization to focus on its core business [15].

2.2 ISO 27001 Standard

ISO/IEC 27001:2022 *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*, is the most well-known standard in the ISO/IEC 2700x standard family for ISMS. It is developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). [2, 15, 17] The latest version was published in October 2022 [15, 17]. The standard specifies the requirements for organizations wishing to establish their own ISMS. These requirements cover the establishment, implementation, operation, monitoring, review, maintenance, and continual improvement of an ISMS. [2, 15, 16, 19, 22, 23] The core of ISO 27001 standard is a process for managing risks, as it is a risk-based information security standard [2].

The standard is designed to help organizations create and maintain their ISMS

and can be used by any organization, not only those in the information technology sector [2, 15]. An organization may have its ISMS audited and certified by an independent third party [15, 24]. Certification demonstrates to stakeholders that the organization is capable of managing risks effectively [15]. It also demonstrates that the organization has implemented their ISMS in accordance with the recommendations of the standard [3].

There are several other standards in ISO/IEC 2700x family. These supporting standards are designed to provide guidance and assist organizations in implementing ISO 27001 standard [2]. ISO/IEC 27002 standard provides detailed descriptions of the 93 controls listed in Annex A of ISO 27001 standard [2, 25–29]. ISO/IEC 27003 offers guidance on implementing an ISMS [2, 26, 28]. ISO/IEC 27004 provides guidance for evaluating the effectiveness of an implemented ISMS [2, 26, 30]. ISO/IEC 27005 is a standard focused on information security risk management [2, 26, 28, 31–33].

2.2.1 Evolution of Information Security Management System Standards

The origins of ISMS can be traced back to the late 1980s, when the first notions of best practices for security controls began to emerge in the UK and the USA [2]. In 1989, the UK Department of Trade and Industry (DTI) published the first code of practice for information security [17, 19, 23]. A subsequent "code of practice for information security management" was introduced in 1993 [23, 24]. This document was named as BSI-DISC-PD003, referring to British Standards Institution-Delivering Information Solutions to Customers-Public Document [17].

In the early 1990s, the UK government established a working group to develop best-practice security guidance for organizations of all types [2, 26]. This effort led to the creation and adoption of BS 7799-1 in 1995, a code of practice for information

security management [2, 19, 23, 24, 26]. A second standard, BS 7799-2 was published in 1998 [23]. Its purpose was to define requirements organizations needed to meet in order to have their ISMS certified [2, 17, 23, 26].

In 2000, BS 7799-1 was submitted to ISO/IEC and subsequently published as ISO/IEC 17799 [2, 17, 19, 26]. It was renumbered to ISO/IEC 27002 in 2006 [2, 26]. This marked the beginning of the ISO/IEC 2700x family of standards, which continues to evolve [2, 17]. In 2005, BS 7799-2 was adopted by ISO/IEC and renumbered as ISO/IEC 27001 [2, 17, 19, 23, 24, 34]. A revised version ISO 27001 standard was published in 2013, and the most recent version was released in 2022 [17]. As history shows, the standard has undergone several revisions. Because the field of information security is constantly evolving, the standard must continue to adapt to new developments.

2.2.2 Plan-Do-Check-Act (PDCA) model

The ISO 27001 standard provides a structured process for establishing, implementing, maintaining, and continually improving an ISMS. This process is known as the Plan-Do-Check-Act (PDCA) model. [18, 19, 26, 29] The PDCA model is also widely referred to as a continual improvement process model [35].

In the *Plan* phase, policies are defined to achieve the information security objectives set by the organization. Risks are identified, and processes and controls are selected to address the identified risks. [2, 14, 18, 19, 22, 24, 29] In the *Do* phase, the ISMS policies, controls, processes, and procedures defined during planning are implemented. [2, 14, 18, 19, 24, 29, 36]. The *Check* phase involves evaluating how well the implemented controls, processes, and procedures perform in relation to the ISMS policy. Finally, in the *Act* phase, the ISMS is maintained and improved based on identified nonconformities. [2, 14, 18, 19, 24, 29] Regular monitoring, reviews of ISMS performance and effectiveness, and ongoing improvements are essential for

maintaining an adequate level of protection [14, 29, 35]. This continual improvement cycle is the core purpose of the PDCA model.

2.2.3 Structure of the ISO 27001 Standard

The ISO 27001 standard consists of 11 sections, or clauses, that are numbered from 0 to 10, as well as one annex [3, 16, 17]. The sections are introduction, scope, normative references, terms and definitions, context of the organization, leadership, planning, support, operation, performance evaluation, and improvement. The annex, known as Annex A, contains a list of 93 controls that are implemented as necessary to meet the requirements of the standard. [3, 16] These controls are discussed in more detail in Section 2.2.4.

Clauses from 4 to 10 constitute the main clauses and mandatory requirements of the standard [3, 16, 17]. They are designed to address all aspects of the ISMS [17]. Without implementing and maintaining all of these clauses, an organization cannot obtain certification [3]. The main clauses are briefly described below [3, 16–18]:

- **Clause 4: Context of the organization**, addresses understanding the organization and its environment, identifying internal and external issues affecting information security, determining the needs and expectations of interested parties, and defining the scope and applicability of the ISMS.

- **Clause 5: Leadership**, requires top management of the organization to demonstrate leadership and commitment to the ISMS, establish an information security policy, and define roles and responsibilities related to information security.

- **Clause 6: Planning**, describes how to assess information security risks and opportunities, set ISMS objectives and plans for achieving them, and plan changes to mitigate risks and pursue opportunities.

- **Clause 7: Support**, concerns providing sufficient resources for the ISMS, ensuring that employees are competent and aware of policies and their responsibilities, managing relevant communication, and maintaining necessary documented information.

- **Clause 8: Operation**, provides guidance for the operational implementation and management of the ISMS. It includes implementing and controlling processes needed to meet requirements, performing risk analysis, creating risk treatment plans, and managing changes.

- **Clause 9: Performance evaluation**, focuses on monitoring, measuring, analyzing, and evaluating ISMS performance. It provides instructions for conducting internal audits and for top management to perform periodic reviews.

- **Clause 10: Improvement**, concerns continually improving the ISMS, addressing nonconformities, and taking corrective actions.

2.2.4 Annex A Controls

As mentioned in Section 2.2.3, the second part of the standard is Annex A, which lists 93 security controls forming a best-practices guide [3]. ISO 27002 standard is a code-of-practice standard that supports the implementation of the controls listed in Annex A [2]. It provides more detailed descriptions of each control [25].

The 93 controls are organized into four themes based on their focus area, and each theme is numbered from A.5 to A.8 [3, 17, 25]. The themes are briefly described below [3, 17, 25]:

- **A.5 Organizational controls**, consists of 37 controls. These controls focus on defining roles and responsibilities, managing risks, and ensuring compliance with legal and regulatory requirements. Their purpose is to guide the behavior of individuals, software, hardware, and systems at an organizational level.

- **A.6 People controls**, consists of 8 controls. Their aim is to ensure that employees comply with standards by acquiring relevant knowledge, training, skills, and experience. They also help reduce human errors and insider threats.
- **A.7 Physical controls**, consists of 14 controls. These focus on physical security and aim to ensure that physical environment is protected and that physical assets are handled securely and appropriately.
- **A.8 Technological controls**, consists of 34 controls. As the name suggests, these are technical controls implemented through software and hardware. Their goal is to ensure the security of information systems through technical measures.

2.2.5 Core Requirements of the ISO 27001 Standard

According to Ganji et al. [19], there are 22 requirements for implementing an ISMS based on the ISO 27001 standard. For example, an organization must conduct a risk assessment in accordance with the standard's requirements [2]. The requirements also cover establishing, implementing, operating, monitoring, reviewing, maintaining, and continually improving the organization's ISMS [15, 16, 19, 27]. Pandey et al. [26] emphasize that there must be commitment from management in the form of analyzing risks and threats and ensuring the logical implementation of security controls. Humphreys [2] also notes that appropriate controls must be selected from Annex A to reduce risks identified during the risk assessment. None of the requirements can be excluded when an organization claims conformity with the standard [19].

One of the core requirements is the Statement of Applicability (SoA) document, which the organization must prepare [27, 37]. The SoA serves as the main connector between the risk assessment and the implemented information security controls

[27]. It must include all the necessary controls from Annex A, justification for their inclusion, whether they have been implemented, and justification for excluding any controls [16, 27, 37]. A well established SoA supports the organization in implementing the required controls effectively into their environment [27].

Management commitment is another essential requirement [16]. Continuous monitoring and improvement of the ISMS is also mandatory [19]. Policy documents form a key component of the organization's ISMS and must address all controls listed in the SoA [16, 19]. Although cultural change is not explicitly listed as a requirement, a survey conducted in 2007 found that 56 % of participants identified cultural change as the main challenge in achieving certification [23].

2.2.6 Certification Process

ISO 27001 conformance can be demonstrated in three ways. They are called first-party assessment, second-party assessment and third-party assessment. A first-party assessment is performed by the company itself. A second-party assessment is performed by a customer or by an auditing company on the customer's behalf. A third-party assessment is performed by a Certification Body (CB). [2] ISO maintains a list of Registered Certification Bodies (RCB) authorized to issue certificates [3, 24]. A first-party assessment is required to demonstrate internal conformance with ISO 27001 requirements, but formal certification is obtained through a third-party assessment, also known as a certification audit. [2] A certificate provides assurance to the organization and its customers that the ISMS meets the requirements of ISO 27001 standard and is systematically reviewed [2, 3, 14, 38, 39].

There are multiple reasons why an organization may seek certification. Certification strengthens organizational structure [3, 39]. It helps avoid regulatory penalties and reduces the need for frequent external audits [3]. Certification adds value to certified organizations because it is granted by independent, recognized certification

body and serves as credible evidence of a well-established ISMS. Although certification requires investment, it often provides a strong return. [2, 38] It reduces the potential financial and reputational impact of cyberattacks [3, 14]. Certificate also reassures stakeholders that the organization is committed to secure business practices [2, 3, 14, 38, 39]. Furthermore, certification may be required by customers or mandated by legislation [2, 39]. In addition, it can provide a competitive advantage [2, 14, 39].

There are two additional parties involved in the certification process aside from the organization seeking certification. These are the National Accreditation Body (AB) and the CB. The AB supervises CBs to ensure that certifications are performed according to requirements set to them. It provides certificates of accreditation to CBs once their certification systems and processes have been successfully assessed. CBs, in turn, evaluate the organization's ISMS and grant certification if the requirements are met. [2]

The first step in the certification process is defining the scope of the ISMS, including initial assessments, requirement analysis, and risk management planning [3, 29]. Before the official certification audit, a pre-certification audit is performed [3, 18, 24, 39]. This helps the organization identify which processes already conform to the standard and which require improvement [3, 24, 39]. In the final stage, the CB conducts on-site audits to verify that the organization's ISMS complies with ISO 27001 standard's requirements [2, 24]. If the organization meets the requirements, the certificate is issued [2, 3, 14, 24, 39]. Follow-up audits are conducted every 6-12 months [2, 3, 18, 24, 39]. These are held to make sure the requirements are still met [2, 3]. The CB may withdraw the certificate if the ISMS no longer meets the standard's requirements [3]. After three years, the organization must undergo recertification to maintain its certification status [2, 3, 24, 39].

2.3 Information Security and Risk Management in IT Infrastructure

It is widely recognized that society is more dependent on information technology (IT), its continuous and reliable functioning, as well as its security, than ever before [40]. Today, companies rely heavily on IT systems to process and manage their data in order to meet their business objectives [41]. Kure et al. [32] note that many critical infrastructures (CIs), such as energy and healthcare, depend heavily on IT to deliver their services securely and reliably. IT forms the foundation of virtually all industries and provides significant advantages to organizations operating in global markets [41]. Consequently, organizations must allocate sufficient resources to information security due to IT's central role in their business and organization [42].

Tripathy [41] states that IT infrastructure is a broad domain composed of diverse components, such as general-purpose computing systems, specialized control systems, communication networks, database management systems, and various software control modules, all of which may potentially be sources of vulnerabilities. While IT provides many benefits, it also brings numerous security threats. Jouini and Rabai [31] and Leitold et al. [43] emphasize that security risks typically arise from compromises to confidentiality, integrity, or availability (CIA). Many cyberattacks are the reason why CIA of critical data is compromised [41, 44]. Information security involves protecting information and IT systems by ensuring confidentiality, integrity, availability, authentication, and non-repudiation [45]. Poor decisions in the design, maintenance, or incident response processes of IT infrastructure may cause severe consequences for an organization's assets, business, individuals, or stakeholders [41, 42].

Turskis et al. [40] mention that many security incidents occur because risks are

either ignored or assessed incorrectly. Understanding the criticality of protecting information and assets is essential for organizations [41]. Organizations must actively manage their cybersecurity risks [32, 41, 42]. Through risk assessments, organizations can identify potential vulnerabilities in their IT infrastructure and make effective business decisions [40, 41]. Kure et al. [32] highlight the importance of risk awareness for selecting appropriate security controls to ensure business continuity. Although risk analysis is costly investment, the long-term benefits outweigh the costs by improving system quality and reliability in the future [40]. Conducting regular security assessments is essential for maintaining effective information security strategies, identifying vulnerabilities, evaluating risks, analyzing threats, ensuring compliance, and applying appropriate security controls to the IT infrastructure. Organizations with continuous and well-structured risk assessment strategies consistently outperform those that are reacting to threats only after they occur. [45]

Leitold et al. [43] mention in their article that measuring the information security posture of an organization is complex due to the lack of objective comparative references. According to Shrivastava [44], the process of risk measurement involves identifying, prioritizing, and evaluating information security risks. Turskis et al. [40] explain that the purpose of risk measurement is to reduce the likelihood of threats and the damage caused by them. Metrics are essential for justifying and directing investments in security [31, 41]. Tripathy [41], identifies vulnerability, exposure, threat and risk as key metrics that management and stakeholders must understand and identify to assess the risks of IT infrastructure. Kure et al. [32], and Santosa and Yusof [45], also identify vulnerability, threat and risk as metrics to be used to assess risks. It is important to define the metrics used in risk assessments [31, 41]. Once risks are identified, necessary remediation strategies can be implemented to mitigate both the probability and impact of risks [41].

Turskis et al. [40] identify four primary risk management strategies that are risk

acceptance, risk mitigation, risk avoidance, and risk transfer to third parties. The chosen strategy depends on the evaluated risk level. Tripathy [41] outlines six steps in an effective risk management process that are evaluation, identification of vulnerabilities, determining exposure, determining threats, assessing risks, and mitigation of risks. Vulnerability management methodologies support security programs by identifying system, application, and network vulnerabilities using automated tools [45]. Organizations may also adopt risk management frameworks to mitigate threats, vulnerabilities, and security risks [31].

The ISO 27001 standard is an example of a risk management framework, as it defines requirements for an ISMS that includes structured and recurring risk assessments, procedures for implementing security controls, and mechanisms for continuous improvement [16, 32, 42, 45]. ISO/IEC 27005 standard provides guidance for organizations on managing information security risks [31–33]. As mentioned in Section 2.2, it supports implementation of the ISO 27001 standard by addressing its risk management requirements [32]. However, ISO/IEC 27005 does not prescribe detailed guidance on how to manage information security risks [31, 32]. Organizations must select an appropriate risk management approach for the scope of their ISMS, industry context, and risk environment [31]. Risk management is one of the foundational requirements for overall security management under ISO 27001 standard [32]. Risk assessments may be quantitative or qualitative [31, 44]. Numerous variables influence risk assessment, including information assets and their criticality, threats, existing controls, identified vulnerabilities, potential incident impacts, and business consequences of incident scenarios [31, 32]. The risk level is determined by assessing both the impact and the likelihood of occurrence [33, 40].

Other proposed risk management solutions also exist. Tripathy [41] proposes a risk assessment solution that calculates threat values for various entities by evaluating their vulnerabilities and exposure levels based on the Common Vulnerability

Scoring System (CVSS). These threat values are counted cumulatively together to produce an overall threat value for an IT system. Kure et al. [32] propose an integrated cybersecurity risk management (iCSRM) framework that uses multiple open security, vulnerability and control repositories such as Common Weakness Enumeration (CWE), Common Attack Pattern Enumeration and Classification (CAPEC), and CIS Critical Security Controls (CSC), along with cyber threat intelligence (CTI) and machine learning models to assess, predict, and manage risks.

2.4 IT Infrastructure Process-Related Controls in ISO 27001 Annex A

This section examines six controls related to processes affecting IT infrastructure. All controls discussed here belong to the technological controls of Annex A [16, 25]. Understanding the requirements of these controls is essential for designing and implementing them later in this thesis. The six controls covered are change management, configuration management, information backup, management of technical vulnerabilities, logging, and monitoring activities.

2.4.1 Change management

Changes occur frequently, especially in organizations operating in the technology sector [46, 47]. Uncontrolled changes to the organization's IT assets, processes, or applications may cause severe harm to business operations [25, 48, 49]. Therefore, a formal change management procedure must be implemented and documented to ensure confidentiality, integrity, and availability during change execution [25]. The objective of change management is to ensure that all changes are secure, auditable, and aligned with information security policies [47]. Change management should be implemented to avoid small changes from causing major risks to security of the

organization [50].

Annex A control 8.32, Change management, of the ISO 27001 standard states that "changes to information processing facilities and information systems shall be subject to change management procedures" [16]. The purpose of this control is to maintain information security during change execution [25, 50]. Change management also helps "minimize disruptions to IT operations" when changes are executed [46]. All changes should be planned, approved, documented, assessed for security impact, communicated to relevant parties, tested, validated, and logged for traceability [25, 47, 49, 50]. A documented rollback method must also exist in case a change fails [25, 48–50]. When executed properly, change management enables organizations to adopt new processes and technologies efficiently [46].

Before implementing a change management procedure, the organization must define what constitutes as a change, who can submit change requests, who can approve them, and who is responsible for implementation [47]. A structured change request form, such as a Jira ticket, should be used to handle changes [47, 50]. At a minimum, the form should include fields for risk evaluation, approval, the nature and purpose of the change, implementation steps, and rollback procedures [25, 47, 50]. It must also be documented that all necessary people are informed about the change [47, 49, 50]. After implementation, the change should be tested and the results documented [47, 50]. Changes should only be implemented to production environment once properly tested and approved [47, 48, 50]. Ideally, the person implementing the change should not be the one approving it [50]. After changes are implemented, they must be monitored to detect unintended security consequences [47, 50].

Auditors expect clearly documented roles related to change management [47, 50]. Proper initiation of change requests is another key audit item [47]. Evidence of a risk assessment must be visible [47, 48, 50]. Changes should be categorized as "Major",

"Minor", or "Emergency" changes [47, 50]. Documented approval demonstrates clear evidence of responsibility in audits [47, 48, 50]. Clearly documented success criteria must be defined to be able to identify if change was successful or not [50]. It must be ensured that proper rollback procedures are documented before a change is approved [48]. Ultimately, successful audit depends on transparent, auditable documentation showing the full lifecycle of each change [47, 48].

2.4.2 Configuration management

Configurations are a fundamental component of hardware, software, and network environments [51, 52]. Configuration management provides the foundation for organization's asset management and system operations [51, 53]. It improves the control, stability, and security of an organization's information assets [53]. Both new and existing systems should fall under configuration management [51]. This control is increasingly automated due to advances in configuration management tools [53]. Maintaining an accurate inventory of all IT assets of the organization is essential for configuration management [53, 54].

Annex A control 8.9, Configuration management, of the ISO 27001 standard states that "configurations, including security configurations, of hardware software, services and networks shall be established, documented, implemented, monitored and reviewed" [16]. The purpose of this control is to ensure secure configurations and prevent unauthorized modifications [25, 48, 51, 54]. It is a preventive control designed to reduce risks [25, 51]. Configuration management commonly includes system hardening [25, 54]. Automation, such as Infrastructure as Code (IaC), should be used in configuration management where possible [25, 53, 54]. Combining IaC with Configuration as Code (CaC), where configurations are treated as code, further enhances automation and security [53]. The Head of IT should act as the owner of the configuration management control [51].

Clear definitions of roles, responsibilities, and processes are important [25, 51]. Security considerations should guide all configuration changes, and publicly available benchmarks or templates should be used to ensure secure baselines [25, 48, 51, 54]. However, organizations must understand their own environments to identify what parts of the benchmarks or templates are applicable to them [48, 51]. Configuration templates should only be accessible to authorized personnel [25, 51]. Configurations must be monitored for unauthorized changes or deviations from baselines [25, 51, 53, 54]. Monitoring should be automated where possible [51, 54]. All configuration changes must follow the change management process [25, 51, 52, 54]. Organizations must also ensure that appropriate licenses exist for configured systems [54].

Organizations should avoid stating that their configurations fully comply with a benchmark or template, as they change and such statements may become inaccurate by the time of audit [48]. Instead, audit readiness requires demonstrating that secure configuration practices are documented, those practices are followed, and configurations are monitored regularly [52–54]. During audits, organizations must show evidence configurations are compared against relevant standards when applicable [48].

2.4.3 Information backup

Backups are essential for organizations because unexpected events can occur, and they must be able to restore information and systems when necessary [55, 56]. There are many possible reasons for this need, such as accidental deletion of data, natural disasters, or ransomware attacks [48, 55]. Therefore, it is necessary to have a proper backup process in place that is regularly tested and ensures reliable recovery [55, 57]. Backups and system restoration are fundamental components of information security and play a key role in maintaining integrity and availability [48, 57].

Annex A control 8.13, Information backup, of the ISO 27001 standard states

that "backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup" [16]. The purpose of the control is to ensure that organizations can recover data and continue business operations if information or systems are lost [25, 55, 57, 58]. It is a corrective control, meaning it is used after something has gone wrong [25, 58]. Organizations should establish a backup policy that considers different types of information and systems [25, 48, 55, 58]. For example, recovery point objectives (RPO) and recovery time objectives (RTO) should be defined based on business requirements [25, 55, 57, 58]. Backup practices should be clearly planned [25]. Also, information should be categorized to ensure it is backed up according to business needs [48, 55–57]. The owner of the information backup control should be the Head of IT or an equivalent role [57, 58].

A variety of backup tasks should be implemented to protect business continuity [48, 57, 58]. Using a backup tool is recommended [55, 56]. It is also important to test backup recovery procedures regularly [25, 48, 55–58]. If a backup is not tested, it is not a backup at all [55]. Backups should be stored securely, in remote locations, and protected through encryption [25, 48, 55, 57, 58]. Automation and monitoring of backup processes are also important [25, 48, 55, 57]. Organizations must also determine appropriate retention periods and delete backups after they expire [25, 55, 57, 58]. Backup requirements apply to cloud systems as well [25, 58].

Documentation plays a critical role in audits and should include legal, regulatory, and contractual requirements for backups [55]. Auditors typically expect evidence that three copies of data exist, they are stored on two different media types, and one copy is stored offsite or in a separate cloud region [55, 57]. They also review documentation of backup policies and procedures [57]. Organizations must be able to demonstrate regular testing of backups [48, 55–57]. One of the most important aspects of an audit is proving that systems can in fact be restored from backups [48,

55, 57]. Missing test logs, insufficient documentation, inconsistent backup schedules, inadequate protection of backup data, or unclear ownership may result in nonconformities in audit [57].

2.4.4 Management of technical vulnerabilities

It is very common for attacks against organizations to exploit known technical vulnerabilities [48]. No IT asset is completely secure, and vulnerabilities are an inherent part of modern network solutions [59, 60]. While strong passwords and firewall rules can prevent some threats, others require more complex measures [61]. Organizations must therefore be able to identify technical vulnerabilities in their systems and take appropriate action before it is too late [48, 59, 61–63]. Investing in vulnerability management is beneficial because early detection and remediation reduce financial impact [61].

Annex A control 8.8, Management of technical vulnerabilities, of the ISO 27001 standard states that "information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken" [16]. The purpose of this control is to ensure technical vulnerabilities are not exploited against the organization [25, 59, 60, 62]. It is a preventive control [25, 59, 60]. Effective vulnerability management helps preserve the confidentiality, integrity, and availability of sensitive information [61]. The process can be treated as a sub-process of change management and therefore it may use existing change management processes that are already established [25, 59, 60]. It is also related to access control and incident management [59–61]. Management of technical vulnerabilities control should be owned by the Head of IT or a similar role [59, 60].

Maintaining an up-to-date inventory of IT assets is essential for effective management of technical vulnerabilities [25, 59–62]. Roles and responsibilities must be

defined [25, 48, 59–62]. A timeline for remediation activities should also be established [25, 48, 61, 62]. Using scanning tools to identify vulnerabilities is also encouraged [25, 48, 59, 61–63]. Organizations should also consider penetration tests and vulnerability assessments to identify potential technical vulnerabilities [25, 48, 61, 62]. Risks associated with discovered vulnerabilities should be assessed, and appropriate actions taken [25, 48, 59–62]. Vulnerabilities should be assessed using a standard scoring system such as CVSS, and those posing the highest risk to the organization's business should be remediated first [61, 62]. Vulnerability remediation should be linked to the change management process, and information backup to ensure planned changes and possibility to revert changes in case they fail [25, 48, 62]. In urgent cases, fixing vulnerability may need to follow the incident management process [25, 61]. If no patch is available, organizations may apply temporary workarounds or disable affected services [25, 59, 60]. Vulnerability information should be obtained from manufacturers and other trusted sources [25, 62, 63]. Establishing a public contact point or bug bounty program for security professionals to report vulnerabilities in organization's systems or products may also help identify vulnerabilities [25, 59, 60, 62].

During audits, the organization's vulnerability practices are evaluated [48, 62, 63]. Auditors check that a clear management process for technical vulnerabilities exists [48, 59, 60]. The process should also be periodically reviewed for improvements [59–62]. Organizations must analyze their exposure to identified vulnerabilities and present evidence about that during the audit [63]. Clear audit logs demonstrating how technical vulnerabilities are managed must be available [25, 59–63]. Evidence of testing and retesting is important to confirm that remediation was effective [48, 61]. Auditors will also require evidence of risk assessments of unpatched vulnerabilities [62]. Records of vulnerability analyses and mitigation actions form key audit evidence [61].

2.4.5 Logging

Having logs greatly supports the identification of incidents and is essential during investigations [48, 64]. Logs provide a comprehensive view of what is happening within an organization's IT infrastructure [64–67]. With the help of logs, the sequence of events leading to an incident can be reconstructed, and accountable individuals can be potentially identified [48, 64, 66]. However, organizations typically generate large volumes of diverse log types [25, 48]. Such volumes are difficult to analyze manually, making automation essential in log analysis to identify meaningful events [25, 48, 64]. It is crucial that organizations produce log data that is accessible and can be efficiently analyzed [65].

Annex A control 8.15, Logging, of the ISO 27001 standard states that "logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analyzed" [16]. Its purpose is to ensure organizations collect, store, and analyze logs properly in order to gather evidence, identify incidents, and support investigations [25, 64, 65]. The control describes main events to log, best practices for protecting logs, and the importance of regular log monitoring [65]. It is a detective control, meaning its objective is to detect potentially malicious activity [25, 64]. In cloud environments, logging responsibilities may be shared between customer and service provider [25, 65]. The logging control should be owned by the Head of IT or an equivalent role [65].

Log collection should be based on the organization's risk assessment and contextual requirements [25, 48, 64]. Responsibilities and time to analyze the produced logs must be assigned [48]. Logged events should include, when applicable, user identifiers, activities, timestamps, device identifiers, and network statistics [25, 64, 65]. Different types of events, such as successful and failed logins, changes in configurations, and use of privileged accounts, should be considered when defining events that are logged [25, 64–66]. Logs must be retained long enough to support poten-

tial investigations and must be protected from unauthorized modification [25, 48, 64–66]. Logs are useful only if their integrity can be trusted [48, 65]. For accurate log analysis results, system clocks must be synchronized [25, 65]. Organizations must ensure that logs cannot be tampered with [25, 48, 64–66]. Techniques such as hashing or storing logs in read-only files can help ensure integrity of logs [25, 65]. Organizations should also notice that some logs may contain Personally Identifiable Information (PII), so appropriate measures must be taken to protect those logs [25, 64, 65]. Logs must be analyzed and interpreted to identify suspicious activity [25, 64–66]. Potential security incidents identified through log analysis should follow incident management procedures [25, 66]. The monitoring activities supports the log analysis process [25, 64–66].

During an audit, auditors will check that a logging policy specifying what logs must be collected is in place [48, 64]. They will also verify that logs are collected at an appropriate level of detail [48, 67]. Organizations must demonstrate that privileged users cannot modify logs generated by their own activities [64]. Auditors will expect evidence that relevant logs are collected [48, 64, 67]. They must confirm that organization has defined log retention and protection measures and with random selection from logs ensure that these definitions are followed in practice [48, 64, 66]. Log review frequency will also be examined during audit [48, 64]. Auditors will review the use of automated log-handling tools and inspect log events that triggered corrective actions [48]. Organizations must also provide evidence of internal audits related to logging [64].

2.4.6 Monitoring activities

Monitoring is important for organizations to identify potentially malicious activity on organizational networks [25, 68, 69]. Monitoring provides visibility into systems, helping organizations understand what is happening, when, and by whom [66]. Or-

ganizations must detect potential attacks before they escalate into incidents [48]. Organizations should also focus on monitoring communications to identify botnets and take necessary actions [25]. Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and Security Incident and Event Monitoring (SIEM) systems are common monitoring solutions [48].

Annex A control 8.16, Monitoring activities, of the ISO 27001 standard states that "networks, systems and applications shall be monitored for anomalous behavior and appropriate actions taken to evaluate potential information security incidents" [16]. Its purpose is to help organizations detect potentially malicious activity and security incidents [25, 66, 68–70]. It emphasizes both proactive and reactive approaches to threats and events in IT infrastructure [66, 68, 70]. The goal is to prevent incidents before they occur [66, 68–70]. It is both a detective and corrective control [25, 68, 70]. Although monitoring and logging are closely related, monitoring is considered an active control, whereas logging is a passive one [68]. The monitoring activities control should be owned by the Head of IT or an equivalent role [70].

The scope of monitoring must be defined based on organization's business and security requirements, as well as laws and regulations affecting the organization [25, 48, 70]. Monitoring and logging are interconnected, as monitoring is largely based on logs [25, 66, 70]. Like logging, monitoring may also be overloaded by huge number of irrelevant events, and therefore, it must be defined what to monitor, how monitoring is performed, and why monitoring is needed [48, 68]. Monitoring may also cover other things such as network traffic, login activities, and configuration files [25, 68, 70]. Risk assessment plays an essential role in designing monitoring activities [48, 68]. It is essential to understand what activities are considered normal in order to identify potentially malicious activities [25, 48, 68, 70]. Alert thresholds should be configured based on the organization's risk appetite, vendor recommendations, and available threat intelligence [48, 68]. Using some kind of monitoring tool should

be considered to ensure continuous monitoring [25, 66, 68–70]. The chosen tool should be able to handle large amounts of data, detect different types of events, and issue alerts for suspicious activity [68, 70]. Employees must be trained to handle alerts created by the monitoring system [25, 66, 68, 69]. Monitoring must also comply with data protection laws, and employees must be clearly informed what is monitored [68]. Continuous improvement of monitoring is essential to reduce false positives [25, 66]. It should also be improved to respond to the rapidly evolving threat landscape [48, 66, 68].

Auditors will review risk assessments related to monitoring [48]. Documentation and evidence of internal audits must be available [68]. Alerts, incidents, and event histories must be traceable [48]. Auditors will expect evidence that all necessary assets are monitored [48, 68]. They will also review how incidents were detected and handled [48, 68, 69]. Auditors also evaluate whether monitoring increases the organization's security and supports their risk appetite [48, 68]. Organizations should be prepared to explain how incidents detected outside office hours are handled [48].

2.5 Implementation Considerations for On-Premises and Cloud Environments

There are several factors to consider when implementing controls in both on-premises and cloud environments. First, the use of security tools should be evaluated, as they can significantly enhance security of IT infrastructure [42]. Such tools include vulnerability scanners, penetration testing frameworks, SIEM platforms, and risk management systems [45]. Organizations should also take advantage of logging and reporting solutions [31]. The use of advanced encryption, multi-factor authentication, access control mechanisms, and automated monitoring reduces the risk of unauthorized access and other security threats, while also supporting development

of robust IT infrastructure that supports business processes and evolving technology while making sure that regulatory requirements are followed [71]. Santosa et al. [45] emphasize the importance of comprehensive planning, stakeholder engagement, and clear implementation strategies that align with organization's business objectives and available resources in order to successfully implement a security assessment program. Regular monitoring and audits allow organizations to identify potential vulnerabilities in their IT infrastructure in a timely manner [71]. When selecting and deploying assessment technologies, organizations must consider scalability, integration capabilities, reporting features, and compatibility with the existing IT infrastructure [45].

It must also be ensured that data stored in the cloud remains confidential and that its use is monitored [31]. Organizations can utilize cloud-based solutions that automatically collect and analyze logs to reduce both operational and human-related risks [71]. Ensuring that the cloud service provider uses multi-factor authentication is important for security [31]. Backups of information, applications, and systems are also necessary in cloud environments, and organizations must plan how to meet backup requirements [25]. When using Infrastructure as a Service (IaaS), encryption must be used to protect against offline attacks [31]. Security and accessibility of cloud environments can be improved by mitigating risks and errors that may affect organizational operations [40]. However, ensuring integrity, availability, and privacy is often more challenging in cloud environments because services and data are often handled by a third party [31].

3 State of the Current IT Infrastructure

In this chapter, the current state of the target organization's IT infrastructure and the existing processes are described. In addition, the risks identified due to insufficient controls are discussed at a general level. At the end of the chapter, a gap analysis between the current and target situations is presented.

3.1 Current IT Infrastructure

The IT infrastructure of the target organization can be divided into two groups. The first group is the on-premises infrastructure, and the second is the cloud infrastructure. The on-premises infrastructure includes all devices that are physically located at the organization's premises. This physical location refers their office. This infrastructure can be further divided into two layers. The first layer consists of the physical hardware devices located on site. The second layer consists of the virtual infrastructure hosted on this physical hardware.

Several infrastructure devices are in place to manage security and network functions. The target organization uses a firewall to block unwanted network traffic. Multiple switches are used to forward traffic in local network, and their configuration follows the Spanning Tree Protocol (STP). STP is a network protocol designed to create a loop-free network topology while maintaining connectivity between Local

Area Networks (LANs) [72]. There are also multiple storage units for data storage, and hosts for running virtual servers in a virtualized environment. In addition, the target organization operates some physical servers. Uninterruptible Power Supplies (UPS) are used to ensure that, in the event of a power outage, systems can remain operational long enough to allow for a graceful shutdown.

The second group consists of cloud infrastructure. The target organization uses several cloud service providers, although the current cloud environment is relatively small. In the cloud, the target organization operates virtual networks and virtual servers, most of which are used for development purposes. Network segmentation is also applied in the cloud environment.

The target organization maintains both internal and guest networks. The internal network is segmented into several network segments to reduce the risk lateral movement in case an intruder gains access to its network. Virtual networks also exist within the virtualized environment. Access to the internal network requires a certificate, while the guest network is protected with a password. In addition to wired Ethernet connectivity, the target organization operates a Wireless Local Area Network (WLAN) with multiple access points. Furthermore, a Virtual Private Network (VPN) is available for employees to securely connect remotely to the target organization's internal network.

3.2 Existing Risk Management and Security Practices

The existing processes of the target organization are described below. These are divided into sections based on the controls to which they relate. The current processes are presented without excessive detail in order to maintain the operational security of the target organization.

Change Management

Currently, there is no clearly defined process for managing changes. Changes are implemented whenever they are considered necessary. In some cases, a ticket is created to document the change, but this is not mandatory. The IT department of the target organization decides on changes to the IT infrastructure, but there is no official authorization mechanism, making it impossible to audit who approved a given change. Documentation of changes is inconsistent. Larger changes are usually documented, but documentation is not integrated into a formal change management process. Many of the activities typically included in a change management process are performed informally within the target organization. The main issue is the absence of a standardized, repeatable process that is consistently followed whenever a new system is introduced or major modifications are made to an existing system.

Configuration Management

Due to the lack of a formal change management process, configuration changes are also not managed in a structured way. As a result, configuration changes cannot be audited. Changes are made when considered necessary, but they are not authorized through a defined process. Furthermore, configurations are not monitored for unauthorized modifications. Configuration changes may be planned before implementation, but no written plan exists. Configuration changes are tested after implementation, but no written test plan exists. Additionally, configuration changes are made directly in the production environment because the target organization does not have a dedicated test environment for IT infrastructure. Configurations are generally based on security baselines provided by manufacturers or on Center for Internet Security (CIS) benchmarks when available and applicable.

Information Backup

Information backup is handled relatively well in the target organization. All critical systems and services are included. Some systems are backed up daily. Also, backups are taken before major updates are applied to systems or services. For the most critical systems, the Recovery Point Objective (RPO) is set to one business day. RPO is defined as the maximum amount of data that may be lost when the most recent backup is successfully restored, and it is measured in units of time [73].

For less critical systems, the interval between backups may be as long as six months. For example, an Open Virtualization Format (OVF) template of the Virtual Machines (VMs) running in the organization's virtualization environment is manually created every six months by the IT Manager of the target organization. The target organization has not defined Recovery Time Objective (RTO). RTO represents the maximum acceptable downtime for restoring a system or service [73]. For the most critical systems, the implicit RTO appears to be one business day, although this is not formally documented.

IT infrastructure configuration backups are stored in a cloud-based version control system. Some backups are stored in on-premises storage and uploaded to the cloud weekly, where they are encrypted. Weekly copies are also saved to an offline external hard drive protected with encryption.

Management of Technical Vulnerabilities

The target organization does not have a clearly defined process for managing technical vulnerabilities. A ticket may be created for a vulnerability fix, but this is not mandatory. The absence of a formal change management process also negatively affects vulnerability remediation. Vulnerabilities are identified through Microsoft Defender, manufacturer vulnerability advisory emails, or emails from the National Cyber Security Center (NCSC). Microsoft Defender does not cover all IT infras-

tructure devices and detects vulnerabilities only in software components. Servers are updated once per month unless a critical vulnerability is discovered and a fix is available. Other devices are updated when vulnerabilities are identified and patches are available. However, risks associated with vulnerabilities are not evaluated in a structured way.

Logging

The target organization does not currently use centralized logging for IT infrastructure devices. Many devices generate local logs, but these logs are not forwarded for automated analysis. Some devices do not have logging enabled at all. Certain protective mechanisms exist to prevent unauthorized access to logs, but there is no monitoring to detect potential tampering. Log retention periods are also undefined.

Monitoring Activities

The target organization has a lightweight monitoring system in place for most IT infrastructure devices, checking only whether devices respond. Some devices are monitored more closely than others depending on their capabilities. The monitoring software sends email alerts if unusual conditions are detected, such as a device not responding to ping. However, logs generated by infrastructure devices are not automatically monitored, and anomalies are not identified from log data. There is no established process for manual monitoring of devices or their logs. Microsoft Defender is used to some extent, but its visibility into IT infrastructure devices is currently very limited. Monitoring for UPS devices is implemented separately to provide alerts regarding power outages.

3.3 Identified Risks and Vulnerabilities

Next, the identified risks and vulnerabilities are described at a general level. These cannot be presented in detail in order to maintain the operational security of the target organization. The risks and vulnerabilities discussed below arise from the absence of proper security controls.

Change Management

The lack of a proper change management process introduces several risks. It may affect the confidentiality, integrity, and availability of information. Because there is no authorization process for changes, it is not possible to determine which changes are authorized and which are not. This creates a risk of unauthorized changes going unnoticed. Although relevant personnel are often informed about changes, this is not part of a formal process, meaning there is a risk that communication does not occur. This may lead to confusion and unnecessary workload when investigating why a system is no longer functioning as expected.

Risk evaluation, implementation plans, test plans, and back-out plans are not part of the current change management process. As a result, changes may be implemented without understanding the risks they pose, may be poorly executed or inadequately tested, or may even fail entirely without a plan for reverting them. Although changes are usually performed carefully, the lack of documentation increases the likelihood that changes will not implemented consistently when performed by different individuals. Uncoordinated changes can also result in extended system downtime.

Configuration Management

With the current configuration management practices, a malicious actor could modify configurations without being detected for a long time. This is due to missing

configuration monitoring. Even though configuration changes are typically performed with care, the lack of a formal change management process increases the risk of errors during configuration changes. There is also no clearly documented process to follow when performing configuration changes, which increases the risk of something critical not considered during configuration changes.

Configurations are usually created and modified based on benchmarks and baselines, but since the process undocumented, there is a risk that some configurations remain insecure because security best practices are overlooked. Missing process documentation also increases the likelihood of human error, as individuals may forget essential steps that should be taken when performing configuration changes. Poorly implemented configurations can lead to system malfunctions or insecure system states.

Information Backup

Although the target organization has a relatively strong backup routine, some risks remain. The most significant risk arises from the fact that backups are not regularly tested. This creates a risk that systems cannot actually be restored from backups if needed. Another risk is that the most recent backup may be too old to restore systems to a sufficiently up-to-date state. Not all backups are automated, creating a risk that some backups may simply be forgotten. In addition, some manual backups are currently performed only by the IT Manager of the target organization, and the process is not documented. If another employee must take over, they may not know how to perform the required steps, leading to delays or incomplete backups.

Management of Technical Vulnerabilities

The absence of a clearly defined process for managing technical vulnerabilities creates several risks. First, there is a risk that critical vulnerabilities remain unpatched

because vulnerabilities are not systematically scanned or analyzed. Due to the missing change management process, vulnerability fixes may not be applied in a controlled manner. Testing could also be forgotten because it is not documented as part of any process. Moreover, a fix might introduce unintended side effects that could impact system stability.

There is also a risk that critical systems are not prioritized since systematic vulnerability evaluation is missing. The lack of automated vulnerability scanning increases the risk that vulnerabilities go unnoticed. Collectively, these shortcomings increase the likelihood that a vulnerability is exploited, causing financial losses and impacting business continuity.

Logging

Several risks are associated with the current logging practices. The absence of centralized log collection means there is no clear and centralized visibility across devices, creating a risk that malicious activity goes unnoticed. It also makes monitoring and analysis extremely difficult. Because log retention periods are not defined, there are compliance risks. Logs that should be deleted may be retained too long, or logs that should be kept may be deleted prematurely. Log protection measures are insufficient, increasing the risk that logs could be altered or deleted without authorization. Additionally, because it is unclear which logs should be collected, there is a risk of "log fatigue", where large amounts of irrelevant logs obscure important security events.

Monitoring Activities

Although some monitoring is in place, several risks remain. Not all devices are monitored, creating a risk that malfunctions or malicious actions go unnoticed. The monitoring that is implemented is very limited in scope. The lack of centralized

logging further affects monitoring because alerts may not be generated if logs are not processed. The target organization has not defined the most critical elements to monitor, which introduces the risk that critical systems are not monitored. This may lead to situations where a critical system is down or under attack without being detected.

3.4 Limitations of Existing Controls

To better understand the measures required to comply with the requirements of the ISO 27001 standard, it is essential to identify the gap between the current security practices and the controls mandated by the standard. In this section, a qualitative gap analysis is presented.

Change Management

The gap between the current change management practices and the requirements of ISO 27001 standard's change management control is significant, as the target organization does not have an established change management process. A systematic, documented method for implementing changes is entirely missing. As a result, changes cannot be audited and are not executed in a controlled manner, creating multiple risks. The current situation leaves excessive room for human error and relies heavily on individuals' memory to perform all necessary steps when implementing changes. To meet the standard's requirements, a complete and formal change management process must be implemented. The absence of change management also negatively affects several other controls.

Configuration Management

The largest gap in configuration management arises from the fact that configuration changes are not monitored, meaning unauthorized changes may go unnoticed for

extended periods. Although this is not solely a configuration management issue, the absence of change management contributes significantly to configuration management. Configuration changes are not executed in a systematic or controlled manner, which increases the likelihood of errors compared to configuration changes performed through a formal change management process. While configurations generally follow recognized security best practices, this is not documented. Additionally, configurations are not periodically reviewed to ensure alignment with the latest benchmarks or baselines.

Information Backup

As previously noted in Section 3.2, information backup is handled relatively well in the target organization. Nonetheless, there are gaps that must be addressed to meet ISO 27001 standard's requirements. The standard requires that backups are tested regularly. This is not currently done and it represents the most significant gap in information backup and must be fixed. Some systems should also be backed up more frequently. Although this is a smaller gap, it still needs consideration. While not explicitly required by the standard, some manual backups should be automated to reduce dependence on individual employees. Documentation of backup procedures is fairly good but could be improved to more closely align with the standard's requirements.

Management of Technical Vulnerabilities

There are also several gaps in the management of technical vulnerabilities. First, the target organization lacks a systematic, documented process for vulnerability management. This is a clear gap that must be addressed. A second gap is that not all vulnerabilities are scanned regularly. Although some vulnerabilities are identified through automated scanning tools, they are not analyzed consistently.The absence

of a change management process further affects vulnerability management. There is no defined process for evaluating vulnerability risks, applying fixes, or prioritizing remediation efforts. These gaps must be addressed to comply with the requirements of the ISO 27001 standard.

Logging

Logging contains multiple gaps, with the most significant being the absence of centralized log collection. This greatly complicates other aspects of log management and leads to additional gaps. Regular log analysis is entirely missing and must be implemented to comply with the requirements of the standard. Another major gap is the lack of defined log retention periods, which introduces compliance risks. It must also be clearly defined which logs should be collected to avoid log fatigue and ensure adequate compliance. Furthermore, protection of some logs remains insufficient, representing a minor but important gap between the current and target states.

Monitoring Activities

Although some monitoring activities are already in place, several gaps remain. All IT infrastructure devices should be included in monitoring, and the scope of monitoring should be broader than it currently is. Existing gaps in logging also impact monitoring, as no logs are currently monitored. Log monitoring must be implemented to comply with the standard. Additionally, it is not clearly defined what should be monitored. Documentation is also lacking. It is not documented what is being monitored, what should be monitored, or how monitoring is performed. Addressing these gaps is necessary for better compliance with the ISO 27001 standard.

4 Designing and Implementing Process Controls

The practical part of this thesis involved designing and implementing the six selected controls of the ISO 27001 standard. The design considerations and implementation of these six controls are presented in this chapter. The processes are discussed in detail while ensuring that no confidential information is disclosed.

4.1 Change Management

As discussed earlier in Section 3.4, change management has an impact on multiple controls. Therefore, it is essential to have a well-designed and properly implemented change management process in place. ISO 27001 standard sets several requirements for change management that must be met to comply with the standard, as described in Section 2.4.1. The change management process was designed based on these requirements and the needs of the target organization.

A clear and auditable process for handling changes is necessary. The designed change management process consists of the following steps:

- Creation of a change request, including planning and risk analysis
- Approval of the change
- Informing relevant stakeholders

- Taking backups when possible
- Implementing the change
- Testing to confirm that the change had the intended effect
- Updating documentation
- Closing the change request

Documenting all changes is essential. Barker [50] and Rathod [47] note that a Jira ticket is sufficient for maintaining an audit trail of changes. Since the target organization already uses Jira for various purposes, it was a natural choice for implementing the change management process.

Before implementation, it was necessary to define what types of changes require the creation of a change request. In the target organization, a change request is required for changes that may affect the confidentiality, integrity, or availability of information and that are not considered routine daily tasks of the IT team. Daily IT tasks may occasionally affect information security, but they are treated as pre-approved standard changes. For example, monthly server updates are considered standard changes. Three change levels, major, minor, and emergency, were defined as follows:

- **Major:** a high-risk, high-impact change requiring careful planning
- **Minor:** a low-risk, limited-impact change
- **Emergency:** an urgent change required immediately to address a critical incident or security threat

The change request form was implemented as a Jira ticket with the following fields:

- Title
- Change category (Infrastructure change, Configuration change, Other)
- Change reason (Repair, Upgrade, Maintenance, New functionality, Security, Other)
- Change description
- Change level (Major, Minor, Emergency)
- Risk level (Insignificant, Greater than insignificant)
- RiskID (displayed only if Risk level is set to Greater than insignificant)
- Risk evaluation (displayed only if Risk level is set to Insignificant)
- Implementation plan
- Test plan
- Back-out plan
- Approver

All fields must be filled in before the change request can be submitted. The form ensures that all relevant aspects of the change are considered. The change is briefly described, and its risk and potential impact are assessed. If the change is deemed riskier, a separate risk evaluation is created in the target organization's risk register. Implementation, testing, and rollback plans are prepared in advance, and an appropriate approver is selected.

The workflow associated with the ticket is designed to ensure that all necessary steps are completed. The workflow is shown in Figure 4.1. First, the change request must be approved. The approver may also decline the change request. If the request

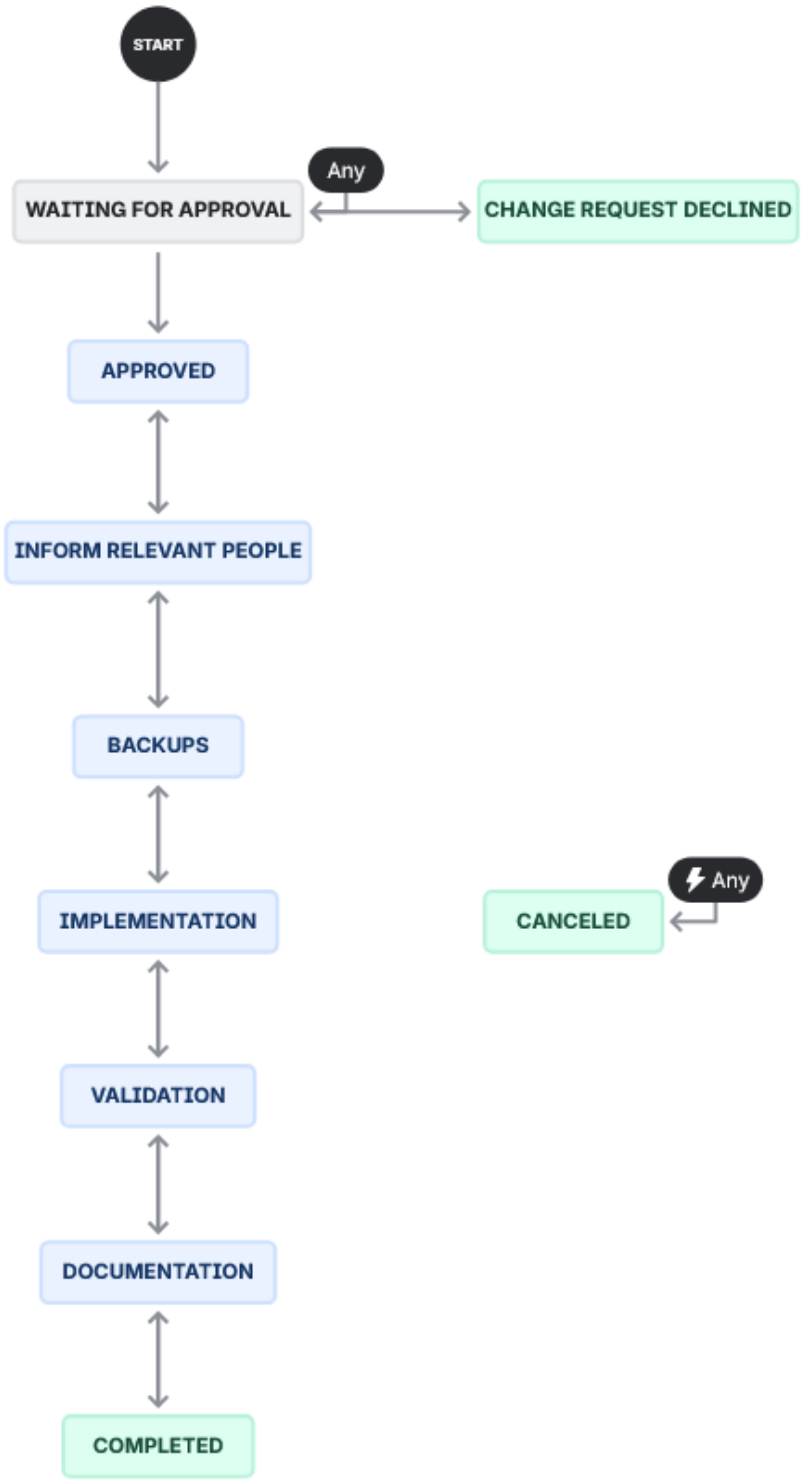

Figure 4.1: Change management workflow

is approved, relevant stakeholders are informed, and backups are taken when possible

to allow for rollback if the change fails. Next, the change is implemented, tested, and validated to ensure that it had the expected effect. Documentation is then created or updated as needed. Finally, the change is marked as completed. The process also allows cancellation of the change at any stage.

The ISO 27002 standard [25] states that changes should be tested in an environment completely separate from production and development environments. However, this requirement may be somewhat excessive in the context of IT infrastructure. The target organization has only a single IT infrastructure environment, meaning that changes must be implemented directly in that environment. Therefore, having a well-defined and robust change management process is essential to ensure that changes are introduced safely and systematically.

The entire process, including the form fields and workflow, is documented on the Confluence page of the target organization's IT team. The high-level description of the change management process is also included in the target organization's Operations Security Policy.

4.2 Configuration Management

In configuration management, it is important that configuration changes are performed in a controlled manner [16]. Therefore, it is specified that all configuration changes must be handled through the change management process. This requirement was incorporated into the new configuration management process description. Although configurations were already extracted and stored in version control after changes, this practice is now formally documented in the process description. Configuration management primarily required improvements in documentation, but some additions were made to ensure better compliance with the requirements of the ISO 27001 standard.

Monitoring configurations is essential to detect unauthorized changes. Auto-

mated monitoring would be the most effective approach, as it would allow real-time detection. However, until automated monitoring is implemented, manual monitoring is required. The process description states that before any configuration is changed, the current running configuration must be compared with the configuration saved in version control to ensure that no unauthorized modifications have occurred. If no changes are made, configurations must still be manually reviewed at least monthly. Any unauthorized configuration change must be treated as an incident and handled through the target organization's incident management process.

Configurations must be secure and should therefore follow CIS benchmarks and manufacturer-provided security baselines where applicable. It is defined that benchmarks and baselines must be reviewed every six months to ensure they remain up to date and that configurations follow current best practices. The review date must be documented in an Excel file created for this purpose, and a reminder to review benchmarks and baselines has been added to the IT team's shared calendar.

The configuration management process documentation outlines the following considerations when establishing or modifying configurations:

- Minimizing the number of identities with privileged or administrator-level access rights
- Disabling unnecessary, unused, or insecure identities
- Disabling or restricting unnecessary functions and services
- Restricting access to powerful utility programs and host parameter settings
- Synchronizing clocks
- Changing vendor default authentication information, such as default passwords, immediately after installation and reviewing other important default security-related parameters

- Invoking time-out facilities that automatically log off computing devices after a predetermined period of inactivity
- Verifying that license requirements have been met

The above items are taken directly from the ISO 27002 standard [25]. The configuration management process is documented on the Confluence page of the target organization's IT team. The high-level description of the configuration management process is also included in the target organization's Operations Security Policy.

4.3 Information Backup

Information backup was already handled relatively well, so the most important task was to document all procedures comprehensively. The documentation is available on the Confluence page of the target organization's IT team, and the high-level description is included in the target organization's Backup Policy and Information Classification Policy. Some adjustments and improvements were also designed and implemented. In addition to regularly scheduled backups, backups are now formally integrated into the change management process. It is defined that backups must be taken before implementing changes whenever feasible.

Many backups already had an established RPO, but for certain backups the RPO was shortened, and for others it was defined for the first time. The RTO was defined in all cases where it had previously been missing, and it is now documented for every backup. Furthermore, the script responsible for automatically deleting backups that have reached the end of their retention period was updated to cover all applicable backups. The process description now specifies that restoration of systems and services from backups must be tested at least annually, where applicable, and that the date of the most recent test must be recorded on Confluence.

Several automatic backups were already in place. Repository backups have now

also been automated using PowerShell scripts and scheduled tasks. Some manual backup tasks remain, but reminders for these have been added to the IT team's shared calendar so that they do not depend on a single individual. These manual tasks include, for example, copying backups to offline storage and performing backups that cannot be automated or would be very difficult to automate.

4.4 Management of Technical Vulnerabilities

A proper process for managing technical vulnerabilities is essential to keep the target organization's IT environment secure and to prevent exploitation of known technical vulnerabilities. The first step in the process is obtaining information about relevant technical vulnerabilities so that they can be addressed appropriately. It was therefore decided that daily vulnerability emails from National Cyber Security Center (NCSC) and vulnerability advisories from manufacturers should be subscribed to using the IT team's email distribution list. This was implemented to ensure that all relevant personnel receive timely vulnerability information. The process description states that these emails must be reviewed upon receipt and that appropriate actions must be taken.

Another method designed to obtain information about vulnerabilities in the target organization's IT infrastructure is to run a Kusto Query Language (KQL) query weekly. This query provides a list of vulnerabilities identified in devices onboarded into Microsoft Defender, offering an overview of the internal IT infrastructure environment's security posture.

When vulnerabilities are discovered, they must be analyzed and addressed appropriately. For this reason, a clear process was designed and documented. The detailed documentation is available on the Confluence page of the target organization's IT team, while the higher-level description is included in the Risk Management Policy and the Operations Security Policy. The process begins with creating a vulnerability

ticket in Jira if the initial analysis indicates that the vulnerability requires further review. The documentation states that a ticket must be created for vulnerabilities categorized as critical or high severity for which an exploit exists. Tickets may also be created for other vulnerabilities if deemed necessary. The ticket includes the following fields:

- Summary
- CVE ID
- Severity (Critical, High)
- CVSS
- Exploit (Yes, No)
- Affected hardware
- Affected software
- Environment (Production, Development, Other)
- Priority (Critical, High, Medium, Low)

All fields except priority are mandatory to ensure that all relevant information about the discovered vulnerability is captured. This information is needed to analyze the vulnerability and determine appropriate actions. Vulnerability management is closely linked to change management. If a vulnerability requires remediation, a change request must be created and the fix implemented according to the change management process.

The workflow of the vulnerability management ticket is shown in Figure 4.2. The workflow begins with the creation of the ticket. Next, the vulnerability is analyzed. At this stage, it is determined whether the vulnerability poses no risk, whether the

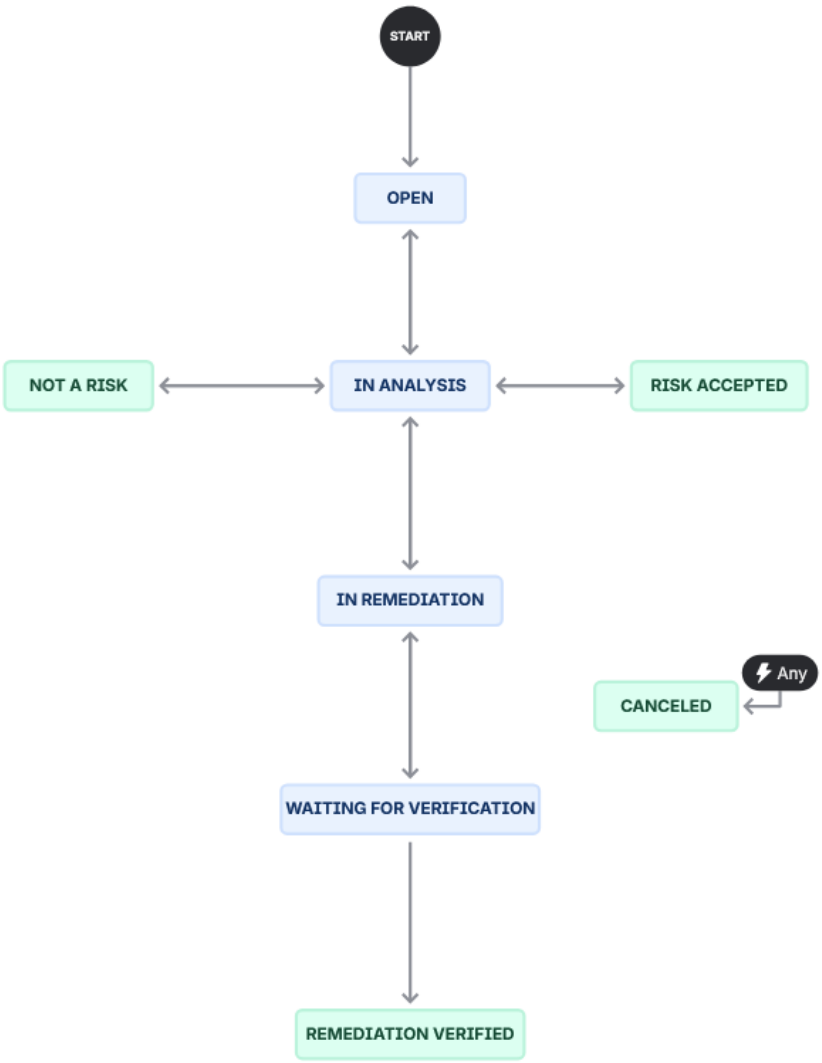

Figure 4.2: Vulnerability management workflow

associated risk is accepted, or whether the vulnerability requires remediation. If a vulnerability is deemed a risk, the workflow requires that a risk entry is created in the risk register and that the corresponding RiskID is added to the ticket. In cases where remediation is required, a change request ticket must be created and linked to the vulnerability ticket, ensuring that remediation is performed according to the change management process. Finally, remediation must be tested to ensure that is successfully addressed the vulnerability. The ticket may be canceled at any time,

but the reason for cancellation must be documented.

4.5 Logging

Due to the complexity and technical nature of centralized logging, the large number of systems involved, and time constraints, the actual implementation of centralized logging was not completed during this thesis. However, a detailed design for the implementation was created. All IT infrastructure log sources were identified, and an analysis was conducted to determine whether and how logs from these systems could be forwarded to a centralized log server for analysis. A centralized log server will be established, and it was defined that a secure connection must be used for all log transmissions. A SIEM system will be utilized to analyze the collected logs.

It must be clearly defined which logs should be collected to avoid log fatigue. Retention periods for all logs must also be established to ensure compliance with relevant regulations. In particular, logs containing Personally Identifiable Information (PII) must be deleted within the required timeframe. It should also be evaluated whether anonymization of such logs is feasible. Documentation of the logging design has been created on the Confluence page of the target organization's IT team, while the high-level documentation is included in the Operations Security Policy.

It was determined that creating a temporary manual process for log analysis is not feasible. The sheer volume and diversity of logs would make manual analysis impractical, potentially requiring multiple employees working full-time in shifts. Therefore, it was concluded that a centralized logging system and automated analysis must be implemented directly, without first introducing a manual interim process.

4.6 Monitoring Activities

The monitoring activities control is closely tied to logging. It is also highly technical and requires significant automation in order to be effective. Therefore, it was decided that, due to time constraints, not all components of the IT environment needed to be brought under monitoring during the timeframe of this thesis. Creating a manual monitoring process would not be meaningful, as it would be too time-consuming. Documentation has been added to the Confluence page of the target organization's IT team, and the high-level description is included in the Operations Security Policy.

A SIEM system is planned to be used for monitoring and analyzing logs once centralized log collection is implemented. All servers were onboarded into Microsoft Defender to improve visibility. While Defender provides some monitoring capabilities, its functionality is still limited, making centralized log collection essential for effective monitoring. When monitoring is implemented, a baseline of normal activity must be established against which monitoring data can be compared. Establishing this baseline in advance is difficult due to limited knowledge of the typical activity patterns in the target organization's IT infrastructure.

5 Evaluation of Implemented Controls

In this chapter, the implemented controls are evaluated. Their effects on the risks identified in Section 3.3 are assessed, and the impacts on process efficiency and potential automation opportunities are examined. A qualitative analysis is used to interpret these effects. This chapter aims to answer all three research questions.

5.1 Change Management

The implemented change management process mitigates many of the risks previously identified. Although it does not fully eliminate all risks, the structured process ensures that changes are implemented systematically and in a controlled manner. Changes are now planned in advance, and the plans are documented. This reduces the risk of poorly planned or improvised changes. Documentation is also beneficial if issues arise later or if similar changes need to be repeated in the future. Testing and rollback procedures are included in the process, requiring the implementer to carefully consider both before executing a change. This mitigates the risk of untested changes and ensures that reverting a change is easier because rollback actions have already been defined.

Previously, unauthorized changes posed a notable risk. With the new approval step included in the process, this risk is mitigated because changes cannot proceed

without proper authorization. The process also requires the implementer to inform all relevant stakeholders, reducing the likelihood that individuals affected by a change are unaware of it. This ensures that employees can prepare accordingly and are not caught by surprise if something functions differently after the change. Another important component of the new process is the mandatory risk evaluation, which helps identify potential risks associated with changes and enables appropriate mitigation actions.

The new process has a noticeable impact on efficiency. Previously, changes were often undocumented or documented only with a simple ticket containing just a summary, a description, and the reporter's name. Creating a change request now takes significantly longer. The exact time depends on the complexity and criticality of the change, but some estimates can be made. The previous ticket type contained three fields, whereas the new one has twelve fields, which is nine more than before. Although this does not necessarily mean that ticket creation takes three times longer, it is clear that the time requirement has increased. Although no data exists on ticket creation times before or after implementation, it can be inferred that the new process has increased the time required.

Another drawback concerning efficiency is the required approval step. In some cases, change requests may be approved almost immediately after creation, but approval might also take hours or days. This can be problematic when a change needs to be implemented quickly. Emergency changes are an exception, as they can be implemented without prior approval. However, for changes not classified as emergency changes, waiting for approval may delay implementation. Validation and documentation are formal parts of the process. Although these activities were performed to some extent previously, their formal inclusion means they must be carried out more thoroughly, which also requires additional time.

It is important to note that despite the negative impact on efficiency, the new

process significantly mitigates earlier risks. The reduction in efficiency is acceptable given the substantial increase in security. It is also likely that the impact on efficiency will decrease over time as employees become accustomed to creating and approving change requests. The new process will eventually become routine.

Automation could help reduce negative effects on efficiency. However, identifying tasks suitable for automation in the change management process is difficult. One possibility is automating approval for certain predefined low-risk changes that still require a change request. On the other hand, such automation may introduce a risk that changes requiring human review are mistakenly performed through automatic approval. Careful consideration would be necessary before implementing any automation in this area.

5.2 Configuration Management

The new change management process mitigates many of the risks previously identified in relation to configuration management. Because configuration changes must now be submitted as change requests with "configuration change" selected as the change category, the risk of uncoordinated configuration changes has been significantly reduced. Configuration changes must be planned in advance, and their testing and potential reversion must be considered before implementation. In addition, all configuration changes require approval, ensuring that another employee reviews the plan before any modification is made.

Previously, configurations were not monitored for unauthorized changes. The new process includes a step that requires comparing the current running configuration to the version stored in version control, helping to identify any unapproved or unintended modifications. It is also specified that configurations must be reviewed at least once a month. These measures collectively reduce the risk of unauthorized changes. Furthermore, a list of considerations must now be applied whenever con-

figurations are created or modified, and the use of benchmarks and baselines has been more strongly integrated into configuration management. These measures help address the risk of insecure configurations. Benchmarks and baselines are to be reviewed every six months to reduce the likelihood of relying on outdated security best practices when establishing or modifying configurations.

The decrease in efficiency largely comes from the new change management process. Configuration changes are subject to the same documentation and approval requirements as other types of changes. Creating the required documentation takes more time than before, and the approval step may introduce delays affecting efficiency, particularly if approval is not granted promptly. Manual monitoring also reduces efficiency. Reviewing all configurations manually each month and performing manual comparisons before changes are implemented require substantial time and effort. Despite this slight reduction in efficiency, overall security has improved due to the structured nature of the new process.

Manual monitoring affects efficiency, and therefore, should be automated. Automating configuration monitoring would remove the need for monthly reviews and pre-change manual comparisons. Several options exist for enabling automation. Commercial tools designed specifically for configuration monitoring could be used. Alternatively, a custom script could be developed to compare the running configurations against the version stored in version control and automatically send alerts to the IT team if differences are detected.

5.3 Information Backup

It is now stated in the process documentation that backups must be tested at least once per year. A table has also been created for recording these tests, providing evidence that recovery procedures are actually verified. The purpose of these measures is to reduce the risk associated with untested system recovery. Although this still

relies on manual testing, it is significantly better than no testing at all. Additionally, RPOs, RTOs, and retention times are now more clearly documented to avoid risks such as being unable to recover data to a recent enough state or storing backups longer than required.

Some backups were already automated prior to implementation of the new control, and additional backups were automated during the process. Automated backups mitigate the risk of human error, particularly the risk of forgetting to take a backup. Not all backups are automated yet, but reminders with detailed instructions have been added to the IT team's shared calendar. These reminders help reduce the risk of missed manual backups and ensure that the knowledge of how to perform them is not held solely by the IT Manager.

The new process does not significantly affect the efficiency of information backup compared with the previous situation. Regular testing is now required, and documenting these tests takes time, but it is difficult to determine whether this has a negative impact on efficiency since testing was not performed before. Because more backups are now automated, the amount of manual work has decreased slightly, improving efficiency. Overall, there are no major efficiency changes compared to the previous state. Information backup practices were already relatively strong and only required the addition of regular testing and some minor adjustments.

One area where automation could further improve efficiency and mitigate risks is automated recovery testing. Automating the restoration tests would allow far more frequent verification, potentially monthly or even weekly, making it possible to detect issues much earlier. Additionally, if technically feasible, the remaining manual backups could be automated. This would further increase efficiency by reducing manual tasks and would nearly eliminate the risk of missing backups due to human error.

5.4 Management of Technical Vulnerabilities

Several risks related to the management of technical vulnerabilities were identified in Section 3.3. The new vulnerability management process is designed to mitigate these risks. It now clearly documents how vulnerabilities should be identified and includes the use of vulnerability scanning queries in addition to reviewing vulnerability emails. These measures reduce the likelihood that vulnerabilities go unnoticed and are not analyzed and fixed. It is now also more systematic how vulnerabilities are discovered compared with the situation prior to the new control. However, there is still a risk that the IT team forgets to run the scanning query and does not analyze the vulnerabilities it identifies in the internal IT infrastructure.

Previously, there was no clear documentation on how vulnerabilities should be handled. It is now defined that vulnerabilities categorized as critical or high, and for which an exploit is available, must be analyzed as soon as possible. A vulnerability ticket must also be created for these vulnerabilities. These steps ensure that vulnerabilities are addressed systematically and reduce the risk of vulnerabilities being ignored. Ticket creation also ensures that the analysis and remediation actions are documented and auditable, reducing the risk of undocumented fixes.

Compared with the previous informal approach, the new process introduces additional steps from the discovery of a vulnerability to its remediation. These steps have a negative effect on efficiency. Previously, vulnerabilities were simply discovered and later fixed depending on an informal, undocumented assessment of their criticality. Now, addressing a vulnerability requires a documented analysis and the creation of a change request. This increases the workload compared to the earlier process. However, these measures substantially reduce risk, making the trade-off between efficiency and security acceptable. The new KQL query improves efficiency slightly by compiling all discovered vulnerabilities into a single list, making it easier to review them compared to manually opening each device in Microsoft Defender to

inspect vulnerabilities.

There are several opportunities for automation. The KQL query should ideally be automated so that its results are emailed to the IT team regularly. This would make it easier to review discovered vulnerabilities and would also reduce the risk of the IT team forgetting to run the query. Automation could be taken even further by automatically generating vulnerability tickets. If technically feasible, the query could be enhanced to perform preliminary analysis and automatically create tickets for vulnerabilities that meet predefined criteria. This would significantly improve efficiency by allowing the IT team to focus directly on analyzing the created tickets rather than manually reviewing query results and creating the tickets themselves.

5.5 Logging

As mentioned in Section 4.5, logging was not implemented during the work conducted for this thesis. Therefore, it is only possible to fully evaluate how the designed logging solution will mitigate the risks identified in Section 3.3 once it is fully implemented. Centralized log collection and analysis will provide comprehensive visibility into activities occurring within the target organization's internal IT infrastructure. Automated analysis will also enable near real-time detection of suspicious events or system outages. Properly defined log retention periods will help reduce compliance risks. Additionally, clearly specifying which logs must be collected will mitigate the risk of log fatigue. Using secure connections for log transmission reduces the likelihood that a malicious actor could intercept or tamper with logs during transfer.

Currently, if logs need to be collected or analyzed, the process must be performed manually. This is inefficient, but it does not represent a decrease in efficiency, as this was already the case before the new control was designed. It is evident that both collection and analysis of logs must be automated. Automation will dramatically increase efficiency. Furthermore, in the context of logging, automation enhances not

only efficiency but also security, as it significantly reduces the risk that important logs are overlooked and enables analysis to occur almost in real time.

5.6 Monitoring Activities

Currently, only limited monitoring is in place, and it does not target activities occurring within the internal IT infrastructure. It is used mainly to check whether devices are up and running. As described in Section 4.6, monitoring activities is closely linked to logging and therefore requires centralized logging to be implemented effectively. The following evaluates how the designed monitoring solution will mitigate the risks identified in Section 3.3 once it is operational.

When monitoring is implemented, it will provide visibility into all IT infrastructure devices, thereby reducing the risk of a malicious actor operating within the network undetected. It is essential to define the most critical systems to monitor so that risks affecting these systems can be mitigated first. Servers are already monitored to a limited extent through Microsoft Defender, which reduces the likelihood of undetected malicious activities on servers. Establishing a baseline of normal activity, against which monitoring alerts are evaluated, will reduce the frequency of unnecessary alerts triggered by normal behavior.

Automation is essential because manual monitoring is not efficient. Alerts for suspicious activities should be generated automatically. Some automated alerting is already available, but several devices remain unmonitored. As with logging, automating monitoring will enhance both efficiency and security, as it reduces human error and improves the likelihood of detecting incidents promptly.

5.7 Summary

The implemented controls mitigate the identified risks effectively. Almost all risks identified earlier are mitigated to at least some extent. The two designed controls, logging and monitoring activities, are also expected to mitigate risks effectively once they are fully implemented. The controls do have some impact on process efficiency, particularly in change management, configuration management, and management of technical vulnerabilities. However, the increase in security is substantial, making the slight decrease in efficiency acceptable.

Several automation opportunities were identified that could further improve efficiency. Among all controls, logging and monitoring activities require the greatest degree of automation in order to be implemented effectively. All three research questions were answered in this chapter.

6 Conclusion

In this thesis, six Annex A controls of the ISO 27001 standard were examined in terms of their effects on risks and process efficiency. Additionally, possibilities for automating parts of the new controls were investigated, as well as how such automation could improve efficiency. The topic of this thesis is relevant because, as described in Chapter 1, the cyber threats faced by organizations have been continuously increasing. Three research questions were formulated and answered in this thesis, all of which were addressed in Chapter 5.

In Chapter 2, a foundation for understanding the ISMS and the ISO 27001 standard was established. The ISO 27001 standard is a cybersecurity standard against which organizations can certify their ISMS. It was found that obtaining the certification can provide organizations with valuable benefits, such as gaining a competitive advantage. Due to these potential benefits and increasing customer requirements, the target organization also chose to implement an ISMS and certify it against the ISO 27001 standard.

Overall, the target organization already had a relatively strong cybersecurity posture. The primary issue was the lack of documentation. Processes existed for various tasks, but they were either undocumented or insufficiently documented. Although the target organization's IT infrastructure is not very large, it consists of many different devices, which had to be taken into account when designing and implementing the controls. Several risks were identified in Section 3.3, and the newly

implemented controls were designed to mitigate these risks.

Chapter 4 described in detail how the controls were designed and implemented. As part of this thesis, six controls were established and documented on the Confluence page of the target organization's IT team. Two new Jira ticket types were introduced to ensure that the documentation requirements of the standard are met. These tickets also help ensure that all relevant aspects are considered when tasks are carried out. The processes were designed based on the requirements of the Annex A controls of the ISO 27001 standard. The objective was to mitigate the identified risks while maintaining process efficiency and addressing the needs of the target organization.

Four controls were fully implemented, and two controls were designed and partially implemented. The goal was for the controls to mitigate the risks identified in Section 3.3 without significantly impacting process efficiency. The effects of the new controls were evaluated in Chapter 5. It was found that most risks were successfully mitigated by the newly implemented controls. Some risks were not fully mitigated, particularly those related to logging and monitoring activities, as these controls were only designed and partially implemented. Their risk-mitigation effects were evaluated based on the assumption that they will be fully implemented in the future.

Some negative effects on efficiency were identified, mainly caused by the additional documentation required for audit purposes. However, these impacts were not major and were deemed acceptable given the significant improvements in security. Several automation possibilities were also identified that could further enhance efficiency. Some of these automation opportunities would also improve security. Implementing these in the future would reduce manual work and strengthen the cybersecurity posture of the target organization.

References

[1] N. Jevtić and I. Alhudaidi, "The importance of information security for organizations", *Serbian Journal of Engineering Management*, vol. 8, no. 2, pp. 48–53, Jan. 2023. https://doi.org/10.5937/SJEM2302048J.

[2] E. Humphreys, "Information security management system standards", *Datenschutz und Datensicherheit - DuD*, vol. 35, no. 1, pp. 7–11, Jan. 2011. https://doi.org/10.1007/s11623-011-0004-3.

[3] T.-S. Junaid, "ISO 27001: Information Security Management Systems", Ph.D. dissertation, Faculty of Computer Science and Engineering, Frankfurt University of Applied Sciences, Frankfurt am Main, Germany, 2023. https://doi.org/10.13140/RG.2.2.36267.52005.

[4] A. Prozorov, "ISO Survey 2024: ISO/IEC 27001 certificates", *Patreon*, Oct. 2, 2025. [Online]. Available: https://www.patreon.com/posts/iso-survey-2024-140260314

[5] CQI | IRCA, "2020 ISO Survey of Management System Standards reveals 17% increase in certifications", *CQI | IRCA*. Accessed: Oct. 24, 2025. [Online]. Available: https://www.quality.org/article/2020-iso-survey-management-system-standards-reveals-17-increase-certifications

[6] American Accreditation Association, "ISO Survey Results of Certifications to Management System Standards", *American Accreditation Association*. Accessed: Oct. 24, 2025. [Online]. Available: https://aaa-accreditation.

org/iso-survey-results-of-certifications-to-management-system-standards/

[7] D. U. Harmes-Liedtke, "QI Data: The ISO Survey of Management System Standard Certifications", *Quality Infrastructure for Development*, Sep. 16, 2020. [Online]. Available: https://qi4d.org/2020/09/16/qi-data-the-iso-survey-of-management-system-standard-certifications/

[8] System Certification Services, "Exciting Time For Assurance, Certification And The Future Of Management Systems Standards", *System Certification Services*. Accessed: Oct. 24, 2025. [Online]. Available: https://systemcertification.co.uk/exciting-time-for-assurance-certification-and-the-future-of-management-systems-standards/

[9] Jasper, "How Many Companies Have Iso 27001 Certification? – Online ISO", *Online ISO*, Dec. 18, 2024. [Online]. Available: https://online-iso.com/iso-14001/how-many-companies-have-iso-27001-certification/

[10] Etteplan, "Etteplan's extensive ISO 27001 certification across its operations is a strategic response to growing regulatory and customer demands", *Etteplan*, Sep. 18, 2025. [Online]. Available: https://www.etteplan.com/about-us/news/2025/09/18/etteplans-extensive-iso-27001-certification-across-its-operations-is-a-strategic-response-to-growing-regulatory-and-customer-demands/

[11] L. Irwin, "SME suppliers demand ISO 27001 certification", *IT Governance Blog*. Accessed: Oct. 25, 2025. [Online]. Available: https://www.itgovernance.co.uk/blog/sme-suppliers-demand-iso-27001-certification

[12] W. Ashford, "Improving security is top driver for ISO 27001", *ComputerWeekly.com*, Aug. 30, 2018. [Online]. Available: https://www.computerweekly.com/news/252447725/Improving-security-top-driver-for-ISO-27001

[13] R. Alavi, S. Islam, and H. Mouratidis, "A Conceptual Framework to Analyze Human Factors of Information Security Management System (ISMS) in Organizations", in *Human Aspects of Information Security, Privacy, and Trust*, Heraklion, Crete, Greece, Jun. 22–27, 2014, pp. 297–305. https://doi.org/10.1007/978-3-319-07620-1_26.

[14] D. Achmadi, Y. Suryanto, and K. Ramli, "On Developing Information Security Management System (ISMS) Framework for ISO 27001-based Data Center", in *2018 International Workshop on Big Data and Information Security (IWBIS)*, Jakarta, Indonesia, May 12–13, 2018, pp. 149–157. https://doi.org/10.1109/IWBIS.2018.8471700.

[15] *Information technology — Security techniques — Information security management systems — Overview and vocabulary*, ISO/IEC 27000:2018, International Organization for Standardization and International Electrotechnical Commission, Feb. 2018.

[16] *Information security, cybersecurity and privacy protection — information security management systems — requirements*, ISO/IEC 27001:2022, International Organization for Standardization and International Electrotechnical Commission, Oct. 2022.

[17] A. A. Alrehili and O. H. Alhazmi, "ISO/IEC 27001 Standard: Analytical and Comparative Overview", in *Advances in Data-Driven Computing and Intelligent Systems*, Goa, India, Sep. 21–23, 2023, pp. 143–156. https://doi.org/10.1007/978-981-99-9524-0_12.

[18] C. Carvalho and E. Marques, "Adapting ISO 27001 to a Public Institution", in *2019 14th Iberian Conference on Information Systems and Technologies (CISTI)*, Coimbra, Portugal, Jun. 19–22, 2019, pp. 1–6. https://doi.org/10.23919/CISTI.2019.8760870.

[19] D. Ganji, C. Kalloniatis, H. Mouratidis, and S. Malekshahi Gheytassi, "Approaches to Develop and Implement ISO/IEC 27001 Standard - Information Security Management Systems: A Systematic Literature Review", vol. 12, pp. 228–238, Dec. 2019. [Online]. Available: https://www.researchgate.net/publication/344073526_Approaches_to_Develop_and_Implement_ISOIEC_27001_Standard_-_Information_Security_Management_Systems_A_Systematic_Literature_Review

[20] A. Prozorov, "ISO 27001:2022. ISMS Documented Information", Tech. Rep., Feb. 21, 2024. [Online]. Available: https://ciso2ciso.com/wp-content/uploads/2024/04/ISMS-Documented-Information.pdf

[21] ISOfocus, "The cyber secrets", Jan. 2019. Accessed: Nov. 26, 2025. [Online]. Available: https://www.iso.org/files/live/sites/isoorg/files/news/magazine/ISOfocus%20(2013-NOW)/en/2019/ISOfocus_132/ISOfocus_132_en.pdf

[22] A. Białas, "A UML Approach in the ISMS Implementation", in *Security Management, Integrity, and Internal Control in Information Systems*, 2005, pp. 285–297. https://doi.org/10.1007/0-387-31167-X_18.

[23] A. Gillies, "Improving the quality of information security management systems with ISO27000", *The TQM Journal*, vol. 23, no. 4, pp. 367–376, Jun. 2011. https://doi.org/10.1108/17542731111139455.

[24] G. Disterer, "ISO/IEC 27000, 27001 and 27002 for Information Security Management", *Journal of Information Security*, vol. 04, pp. 92–100, Jan. 2013. https://doi.org/10.4236/jis.2013.42011.

[25] *Information security, cybersecurity and privacy protection — information security controls*, ISO/IEC 27002:2022, International Organization for Standardization and International Electrotechnical Commission, Mar. 2022.

[26] M. Pandey, S. Kumar, and S. Karthikeyan, "Information Security Management System (ISMS) Standards in Cloud Computing-A Critical Review", in *2013 International Conference on Control Computing Communication & Materials (ICCCCM)*, Aug. 2013. https://doi.org/10.13140/RG.2.1.3687.4649.

[27] J. Stanik and M. Kiedrowicz, "Statement of Applicability as a Key Element of the GIS Certification Process in the Light of Cybersecurity Standards", *GIS Odyssey Journal*, vol. 2, no. 2, pp. 79–92, Aug. 2022. https://doi.org/10.57599/gisoj.2022.2.2.79.

[28] I. Topa and M. Karyda, "From theory to practice: Guidelines for enhancing information security management", *Information and Computer Security*, vol. 27, no. 3, pp. 326–342, Jun. 2019. https://doi.org/10.1108/ICS-09-2018-0108.

[29] L. N. Ferreira, S. M. da Silva Constante, A. M. de Moraes Zebral, R. Z. Braga, H. Alvarenga, and S. N. Ferreira, "ISO 27001 certification process of Electronic Invoice in the State of Minas Gerais", in *2013 47th International Carnahan Conference on Security Technology (ICCST)*, Medellin, Colombia, Oct. 8–11, 2013, pp. 1–4. https://doi.org/10.1109/CCST.2013.6922072.

[30] M. Sadikin, H. Hardi, L. Mitaliska, and R. Yusuf, "Combining ITAF and ISO 27004 to Perform IS Audit in Higher Education Institution", in *International Conference on Recent Innovations in Computer Science and information Technology (ICRICSIT-2015)*, New York, USA, Jun. 5, 2015, pp. 164–169. [Online]. Available: https://www.researchgate.net/publication/282854227_Combining_ITAF_and_ISO_27004_to_Perform_IS_Audit_in_Higher_Education_Institution

[31] M. Jouini and L. B. A. Rabai, "A Security Risk Management Model for Cloud Computing Systems: Infrastructure as a Service", in *Security, Privacy, and*

Anonymity in Computation, Communication, and Storage, 2017, pp. 594–608. https://doi.org/10.1007/978-3-319-72389-1_47.

[32] H. I. Kure, S. Islam, and H. Mouratidis, "An integrated cyber security risk management framework and risk predication for the critical infrastructure protection", *Neural Computing and Applications*, vol. 34, no. 18, pp. 15 241–15 271, Sep. 2022. https://doi.org/10.1007/s00521-022-06959-2.

[33] *Information security, cybersecurity and privacy protection — guidance on managing information security risks*, ISO/IEC 27005:2022, International Organization for Standardization and International Electrotechnical Commission, Oct. 2022.

[34] G. Culot, G. Nassimbeni, M. Podrecca, and M. Sartor, "The ISO/IEC 27001 information security management standard: Literature review and theory-based research agenda", *The TQM Journal*, vol. 33, no. 7, pp. 76–105, Mar. 2021. https://doi.org/10.1108/TQM-09-2020-0202.

[35] E. Humphreys, *Implementing the ISO/IEC 27001 Information Security Management System Standard*, 1st. USA: Artech House, Inc., 2007.

[36] J. Jevelin and A. Faza, "Evaluation the Information Security Management System: A Path Towards ISO 27001 Certification", *Journal of Information Systems and Informatics*, vol. 5, no. 4, pp. 1240–1256, Nov. 2023. https://doi.org/10.51519/journalisi.v5i4.572.

[37] A. Tanovic, A. Butkovic, F. Orucevic, and N. Mastorakis, "The importance of introducing Information Security Management Systems for Service Providers", *Recent Researches In Electrical Engineering*, pp. 267–275, Oct. 2014. [Online]. Available: https://www.researchgate.net/publication/308759843_The_importance_of_introducing_Information_Security_Management_Systems_for_Service_Providers

[38] C. Hsu, T. Wang, and A. Lu, "The Impact of ISO 27001 Certification on Firm Performance", in *2016 49th Hawaii International Conference on System Sciences (HICSS)*, Koloa, HI, USA, Jan. 5–8, 2016, pp. 4842–4848. https://doi.org/10.1109/HICSS.2016.600.

[39] M. Majerník, N. Daneshjo, J. Chovancová, and G. Sančiová, "Design of Integrated Management Systems According to the Revised ISO Standards", *Polish Journal of Management Studies*, vol. 15, no. 1, pp. 135–143, May 2017. https://doi.org/10.17512/pjms.2017.15.1.13.

[40] Z. Turskis, N. Goranin, A. Nurusheva, and S. Boranbayev, "Information Security Risk Assessment in Critical Infrastructure: A Hybrid MCDM Approach", *Informatica*, vol. 30, no. 1, pp. 187–211, Feb. 2019, Publisher: SAGE Publications. https://doi.org/10.3233/INF-2019-1213.

[41] B. K. Tripathy, "Risk Assessment in IT Infrastructure", in *Security and Privacy From a Legal, Ethical, and Technical Perspective*, IntechOpen, 2020, ch. 6. https://doi.org/10.5772/intechopen.90907.

[42] H. Winarno, F. Yasin, M. A. Prasetyo, F. Rohman, M. R. Shihab, and B. Ranti, "IT Infrastructure Security Risk Assessment using the Center for Internet Security Critical Security Control Framework: A Case Study at Insurance Company", in *2020 3rd International Conference on Computer and Informatics Engineering (IC2IE)*, Yogyakarta, Indonesia, Sep. 15–16, 2020, pp. 404–409. https://doi.org/10.1109/IC2IE50715.2020.9274594.

[43] F. Leitold, K. Hadarics, E. Oroszi, and K. Gyorffy, "Measuring the information security risk in an infrastructure", in *2015 10th International Conference on Malicious and Unwanted Software (MALWARE)*, Fajardo, PR, USA, Oct. 20–22, 2015, pp. 93–100. https://doi.org/10.1109/MALWARE.2015.7413689.

[44] A. K. Shrivastava, "The Impact Assessment of IT Infrastructure on Information Security: A Survey Report", *Procedia Computer Science*, 1st International Conference on Information Security & Privacy 2015, vol. 78, pp. 314–322, Jan. 2016. https://doi.org/10.1016/j.procs.2016.02.062.

[45] R. Santosa and Z. B. Yusof, "The Role of Regular Security Assessments in Maintaining Information Assurance Across IT Infrastructure", *International Review of Machine Learning, Artificial Intelligence, and Applied Data Science*, vol. 15, no. 6, Jun. 2025. Accessed: Jan. 25, 2026. [Online]. Available: https://sagegate.net/index.php/IRMLADS/article/view/Santosa2025

[46] ISO, "What is change management: A quick guide", *ISO*. Accessed: Jan. 31, 2026. [Online]. Available: https://www.iso.org/information-security/it-change-management

[47] B. S. Rathod, "ISO 27001 Change Management Policy: A Complete Guide", *Sprinto*. Accessed: Jan. 31, 2026. [Online]. Available: https://sprinto.com/blog/iso-27001-change-management-policy/

[48] B. Kenyon, "TECHNOLOGICAL CONTROLS", in *ISO 27001 Controls A guide to implementing and auditing*, 2nd ed., Ely, United Kingdom: IT Governance Publishing Ltd, 2024, ch. 8, pp. 169–245.

[49] J. Whiting, "ISO 27001:2022 Annex A Control 8.32 Explained", *isms.online*. Accessed: Jan. 31, 2026. [Online]. Available: https://www.isms.online/iso-27001/annex-a-2022/8-32-change-management-2022/

[50] S. Barker, "ISO 27001:2022 Annex A 8.32 Change Management", *High Table*. Accessed: Jan. 31, 2026. [Online]. Available: https://hightable.io/iso27001-annex-a-8-32-change-management/

[51] T. Cane, "ISO 27002, Control 8.9, Configuration Management", *isms.online*. Accessed: Feb. 1, 2026. [Online]. Available: https://www.isms.online/iso-27002/control-8-9-configuration-management/

[52] Advisera, "ISO 27001 Control 8.9 – Configuration management", *Advisera*. Accessed: Feb. 1, 2026. [Online]. Available: https://advisera.com/iso27001/control-8-9-configuration-management/

[53] ISO, "Configuration management: Why it's so important for IT security", *ISO*. Accessed: Feb. 1, 2026. [Online]. Available: https://www.iso.org/information-security/configuration-management

[54] S. Barker, "ISO 27001:2022 Annex A 8.9 Configuration management", *High Table*. Accessed: Feb. 1, 2026. [Online]. Available: https://hightable.io/iso27001-annex-a-8-9-configuration-management/

[55] S. Barker, "ISO 27001:2022 Annex A 8.13 Information Backup: The Lead Auditor's Guide." *High Table*. Accessed: Feb. 2, 2026. [Online]. Available: https://hightable.io/iso-27001-annex-a-8-13-information-backup/

[56] Advisera, "ISO 27001 Control 8.13 – Information backup", *Advisera*. Accessed: Feb. 2, 2026. [Online]. Available: https://advisera.com/iso27001/control-8-13-information-backup/

[57] A. Gupta, "ISO 27001 Backup And Recovery: Best Practices and Key Steps for 2026", *Konfirmity*, Jan. 15, 2026. [Online]. Available: https://www.konfirmity.com/blog/iso-27001-backup-and-recovery-for-iso-27001

[58] M. Jennings, "ISO 27001:2022 Annex A Control 8.13 Explained - ISMS.online", *isms.online*. Accessed: Feb. 2, 2026. [Online]. Available: https://www.isms.online/iso-27001/annex-a-2022/8-13-information-backup-2022/

[59] T. Cane, "Control 8.8, Management of Technical Vulnerabilities", *isms.online*. Accessed: Feb. 6, 2026. [Online]. Available: https://www.isms.online/iso-27002/control-8-8-management-of-technical-vulnerabilities/

[60] S. Peters, "ISO 27001:2022 Annex A Control 8.8 Explained", *isms.online*. Accessed: Feb. 6, 2026. [Online]. Available: https://www.isms.online/iso-27001/annex-a-2022/8-8-management-of-technical-vulnerabilities-2022/

[61] P. Wadhwa, "ISO 27001 Vulnerability Management + (Free Controls List)", *Sprinto*. Accessed: Feb. 6, 2026. [Online]. Available: https://sprinto.com/blog/iso-27001-vulnerability-management/

[62] S. Barker, "ISO 27001:2022 Annex A 8.8 Management of Technical Vulnerabilities: The Lead Auditor's Guide." *High Table*. Accessed: Feb. 6, 2026. [Online]. Available: https://hightable.io/iso-27001-annex-a-8-8-management-of-technical-vulnerabilities/

[63] Advisera, "ISO 27001 Control 8.8 – Management of technical vulnerabilities", *Advisera*. Accessed: Feb. 6, 2026. [Online]. Available: https://advisera.com/iso27001/control-8-8-management-of-technical-vulnerabilities/

[64] S. Barker, "ISO 27001:2022 Annex A 8.15 Logging: The Lead Auditor's Guide." *High Table*. Accessed: Feb. 8, 2026. [Online]. Available: https://hightable.io/iso-27001-annex-a-8-15-logging/

[65] J. Whiting, "ISO 27001:2022 Annex A Control 8.15 Explained", *isms.online*. Accessed: Feb. 8, 2026. [Online]. Available: https://www.isms.online/iso-27001/annex-a-2022/8-15-logging-2022/

[66] P. Wadhwa, "ISO 27001 Logging and Monitoring Policy: Requirements, Objectives, and Best Practices", *Sprinto*. Accessed: Feb. 8, 2026. [Online]. Available:

https://sprinto.com/blog/iso-27001-logging-and-monitoring-policy/

[67] Advisera, "ISO 27001 Control 8.15 – Logging", *Advisera*. Accessed: Feb. 8, 2026. [Online]. Available: https://advisera.com/iso27001/control-8-15-logging/

[68] S. Barker, "ISO 27001:2022 Annex A 8.16 Monitoring Activities: The Lead Auditor's Guide." *High Table*. Accessed: Feb. 10, 2026. [Online]. Available: https://hightable.io/iso-27001-annex-a-8-16-monitoring-activities/

[69] Advisera, "ISO 27001 Control 8.16 – Monitoring activities", *Advisera*. Accessed: Feb. 13, 2026. [Online]. Available: https://advisera.com/iso27001/control-8-16-monitoring-activities/

[70] S. Peters, "ISO 27002, Control 8.16, Monitoring Activities", *isms.online*. Accessed: Feb. 9, 2026. [Online]. Available: https://www.isms.online/iso-27002/control-8-16-monitoring-activities/

[71] Y. Shevchuk, "Risk Management and Compliance Strategies for Legacy IT Infrastructure", *Emerging Frontiers Library for The American Journal of Engineering and Technology*, vol. 7, no. 8, pp. 85–91, Aug. 2025. Accessed: Jan. 25, 2026. [Online]. Available: https://emergingsociety.org/

[72] R. Perlman, "An algorithm for distributed computation of a spanningtree in an extended LAN", *SIGCOMM Comput. Commun. Rev.*, vol. 15, no. 4, pp. 44–53, Sep. 1985. https://doi.org/10.1145/318951.319004.

[73] O. H. Alhazmi and Y. K. Malaiya, "Evaluating disaster recovery plans using the cloud", in *2013 Proceedings Annual Reliability and Maintainability Symposium (RAMS)*, Orlando, FL, USA, Jan. 28–31, 2013, pp. 1–6. https://doi.org/10.1109/RAMS.2013.6517700.