Bachelor's thesis

Information and Communications Technology, Data Networks and Cybersecurity

2024

Magdalena Nygård

Implementing ISO/IEC 27001:2022 in a SME

– A Case Study Using Cyberday

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

Bachelor’s | Abstract

Turku University of Applied Sciences

Information and Communications Technology, Data Networks and Cybersecurity

2024| 50 pages

Magdalena Nygård

Implementing ISO/IEC 27001:2022 in a SME

- A Case Study Using Cyberday

The digital age poses growing threats like data breaches and ransomware, challenging consulting enterprises managing client data. The ISO/IEC 27001:2022 standard offers a globally recognized framework for building an Information Security Management System (ISMS) to enhance data protection, compliance, and customer trust.

This thesis investigates the early implementation of ISO/IEC 27001:2022 in a Finnish IT consulting SME through a qualitative case study. The researcher actively participated in the implementation team, focusing on aligning operations with clauses 4–10 of the standard.

Additionally, the study examines the Cyberday tool's role in streamlining ISO 27001 compliance by automating risk management and document processes, ensuring adherence to GDPR. The findings provide a practical roadmap for SMEs to tackle ISO 27001 implementation and strengthen information security using effective tools.

Keywords:

ISO 27001, ISMS, Cyberday, GDPR, SME, IT Consulting, Risk Management

Opinnäytetyö (AMK) | Tiivistelmä

Turun ammattikorkeakoulu

Tietojenkäsittely

2024 | 50 sivua

Magdalena Nygård

ISO/IEC 27001:2022 -standardin käyttöönotto pk -yrityksessä

- Tapaustutkimus Cyberday -työkalun käytöstä

Digitaalisen ajan kasvavat uhat, kuten kiristysohjelmat ja tietomurrot, haastavat yhä enemmän konsultointiyrityksiä, jotka käsittelevät asiakasdataa päivittäin. ISO/IEC 27001:2022 -standardi tarjoaa kansainvälisesti tunnustetun viitekehyksen tietoturvallisuuden hallintajärjestelmän (ISMS) rakentamiseen, mikä parantaa tietosuojaa, säädösten noudattamista ja asiakastyytyväisyyttä. Opinnäytetyössä tutkittiin ISO/IEC 27001:2022 -standardin alkuvaiheen käyttöönottoa suomalaisessa IT-konsultointialan pk-yrityksessä laadullisen tapaustutkimuksen keinoin. Osallistuttiin aktiivisesti toteutustiimiin, keskittyen yrityksen toimintojen yhteensovittamiseen standardin kohtien 4–10 vaatimusten kanssa. Työssä selvitettiin Cyberday-työkalun roolia ISO 27001 -vaatimusten täyttämisen tukena. Tutkimusmenetelmällä pystyttiin havannoimaan, että työkalu automatisoi riskienhallintaa sekä asiakirjojen luontia ja hallintaa, helpottaen merkittävästi vaatimustenmukaisuuden saavuttamista ja GDPR-säädösten noudattamista. Opinnäytetyön päätelmät esittivät mallin, jonka avulla pk -yritykset voivat hallita ISO 27001 -standardin tuomat haasteet hyödyntämällä tarkoituksenmukaista työkalua.

Asiasanat:

ISO 27001, tietoturvallisuuden hallintajärjestelmä, Cyberday, GDPR, pk-yritykset, IT-konsultointi, riskienhallinta

Content

Figures

Tables

List of abbreviations (or) symbols

Abbreviation	Explanation of abbreviation
Audit	A systematic and independent process for obtaining evidence and evaluating it to determine the extent to which the audit criteria are fulfilled
CIA	Confidentiality, Integrity, and Availability
ECSM	European Cybersecurity Month
ENISA	European Union Agency for Cybersecurity
GDPR	General Data Protection Regulation
in-house	activities that are conducted internally within an organization
InfoSec	Information Security
ISMS	Information Security Management System
ISO	international Organization for Standardization
NIS	Network and Information Security Directive
SME	Small and medium-sized enterprises
SOA	Statement of Applicability
SOP	Security operating procedures

1 Introduction

1.1 Background

In today’s digital landscape, information security is a critical concern for consulting enterprises that handle sensitive client data. ENISA highlights the importance of strong cybersecurity measures in mitigating risks such as data breaches and ransomware attacks, which can have severe financial, regulatory, and reputational consequences. ENISA's Threat Landscape report from 2024 (European Union Agency for Cybersecurity [ENISA], 2024) emphasizes that understanding and addressing evolving threats is crucial for organizations aiming to protect their data and ensure compliance with regulations like the Network and Information Security Directive (NIS2) and EU’s General Data Protection Regulation (GDPR) (European Union Agency for Cybersecurity, 2024; European Union, 2016). Effective risk management and best practices of cybersecurity can significantly enhance operational efficiency and client trust. For consulting enterprises, failing to secure data can result in reputational damage, financial losses, and regulatory penalties. The risks are heightened by increasingly sophisticated threats such as data breaches, ransomware, and complex compliance requirements (International Organization for Standardization [ISO], 2022).

ISO/IEC 27001 offers a globally recognized framework for managing information security risks. It provides organizations with guidance on establishing, implementing, maintaining, and improving an Information Security Management System (ISMS). The certification to this standard helps organizations to protect data, to manage risks effectively, and to demonstrate strong commitment to security. This enhances client trust and ensures adherence to regulatory requirements (ISO, 2022).

The 2022 updates to ISO/IEC 27001 address common security challenges, such as cloud security, data privacy, and remote work. With the growing reliance on cloud-based technologies, the updated standard emphasizes managing risks

related to data sovereignty and third-party controls. It also strengthens privacy safeguards and offer guidance on securing remote work environments, ensuring its continued relevance in today's evolving security landscape (ISO, 2022). ISO/IEC 27001 synergies with the NIS2 directive in the emphasis of cybersecurity, risk management and regulatory compliance. ISO 27001 is a voluntary international standard and NIS2 is a mandatory EU directive (European Union Agency for Cybersecurity, 2024; ISO, 2022).

1.2 Research questions & theoretical background

The thesis examines the theoretical framework of ISO/IEC 27001:2022, focuses on clauses 4 to 10, which are the most important when implementing the standard. A case study was conducted on a Finnish small to medium -sized enterprise (SME) that specializes in IT consulting, the research investigates the challenges faced by this specific SME when adopting the 27001 -standard. The thesis identifies strategies to address the challenges faced during the implementation of the standard. A central question is: What challenges do SMEs face when beginning the process of implementing ISO/IEC 27001:2022, and how can these challenges be effectively addressed?

The implementation process in a SME and the findings of the case study propose a way for achieving ISO/IEC 27001:2022 implementation, integrating the standard's framework with a practical tool called "Cyberday." This approach simplifies the complexities of implementing an ISMS in alignment with the 2022 updates. Cyberday offered action steps and addressed common obstacles. The study aims to support similar SME consulting enterprises in improving their security practices and to foster a good information security culture for long-term benefits. (ISO, 2022).

Consulting enterprises must account for the local regulatory environment (ISO, 2022). For Finnish SMEs, this includes compliance with the GDPR, which mandates strict guidelines on data protection and privacy (European Union, 2016). To align ISO/IEC 27001:2022 implementation with GDPR and NIS2

requirements means to ensure that data protection measures meet both international standards and legal obligations.

1.3 Research methodology

The case study was conducted in a Finnish SME that specializes in consulting on IT related topics. The team is responsible for implementing ISO 27001. This approach provides an in-depth, real-world examination of the challenges and successes encountered during the implementation process. This SME specializes in information technology consulting, they manage sensitive client data on a daily basis, making the adoption of ISO 27001 relevant to ensure integrity, confidentiality, and availability of information (CIA). The CIA triad is a framework for developing security systems, as highlighted by Fortinet. It is frequently used to pinpoint vulnerabilities and form strategies to address them effectively (Fortinet, n.d.).

The methodology followed a qualitative research design, focusing on data collected through direct participation, observations, and documentation analysis. By being part of the team that did the implementation project, the researcher had firsthand access to the implementation process. This allowed a good understanding of the decision-making process, resource allocation, and the day-to-day challenges encountered during the ISO 27001 adoption.

Several data collection techniques were employed:

1. Discussions: Semi-structured discussions with key stakeholders, including top management, the IT department, and other consultants, helped capture different perspectives on the challenges (further discussed in Section 4.3) and benefits (discussed in Section 2.3) of ISO 27001 implementation (Tevora, n.d.; Secureframe, n.d.-a).
2. Document Analysis: A review of internal documentation, including risk assessments, existing policies, and progress reports, was carried out to evaluate the organization's readiness for ISO certification and identify

gaps in the current information security practices (ISO, 2022; Wadhwa, 2024).

3. Direct Observation: Observing team meetings and implementation sessions gave insights into the practical challenges faced during the implementation, including staff training, resource allocation, and the integration of ISO 27001 into the enterprises existing processes (Tevora, n.d.; Wadhwa, 2024).

This case study-based approach allows for a good examination of the factors influencing implementation, with a specific focus on the key clauses of ISO 27001:2022, particularly those relevant to SMEs. The findings from this case study aim to contribute to a broader understanding of how SMEs in Finland can adopt ISO 27001 to manage information security risks and achieve certification.

1.4 Thesis structure

This thesis is structured into two sections to provide an exploration of ISO 27001:2022 implementation in SMEs, specifically focusing on a case study of a consulting enterprise in Finland. The first section (chapters 1-3) dives into the theoretical framework of ISO 27001:2022. This section covers the standard's background, the key clauses (4-10) that are critical for implementation, and the overall importance of an ISMS. The theory section aims to provide the reader with a good understanding of the ISO 27001 standard, its components, and how it helps organizations safeguard sensitive data and ensure compliance with legal and regulatory requirements (ISO, 2022). This part of the thesis also explores the challenges faced by SMEs when adopting such a framework and the necessary steps for achieving certification, particularly focusing on the needs of consulting enterprises (Tevora, n.d.; Wadhwa, 2024).

The second section (chapter 4) of the thesis focuses on the practical application of Cyberday as a tool in the implementation process. Cyberday is a platform designed to streamline the adoption of various frameworks. ISO 27001 was relevant to this specific SME. Chapter 4 will elaborate how Cyberday was

integrated into the implementation process, highlighting the platforms' role in simplifying otherwise complex tasks, such as risk assessments, policy creation, and monitoring (Cyberday, 2024). When combining the theoretical guidelines of ISO 27001 with the practical features of Cyberday, this section aims to show how automated tools enhances the process (Cyberday, 2024).

2 Information Security and ISO 27000 standards

Information security, often referred to as "InfoSec," involves protecting data and information systems from unauthorized access, modification, or destruction (UpGuard, n.d.). Its primary objective is to ensure the confidentiality, integrity, and availability of data, commonly known as the CIA triad (Bunker Your Risk, n.d.).

The importance of information security in today's digital landscape can't be overstated. As reliance on digital platforms for personal, financial, and business data grows, protecting this information is more important than ever before. The rising occurrence of cyber threats like phishing, ransomware, and hacking underscores the need for strong security measures to safeguard various assets and mitigate potential attacks (University of Queensland, n.d.).

Information security is essential for building trust (ISO, 2022). Organizations that prioritize safeguarding user data not only enhance their reputation but also boost confidence among customers and stakeholders. Trust is fundamental for business sustainability, especially in times where data breaches can result in severe reputational harm and financial losses. Additionally, compliance with legal and regulatory frameworks, including GDPR for SMEs in Finland, is a legal requirement (European Union, 2016).

2.1 The ISO 27000 family of standards

The ISO 27000 series represents a globally recognized framework of standards crucial for organizations seeking to strengthen IT security, cybersecurity, and privacy protection (ISMS.online, n.d.). These standards provide a systematic approach to managing information security, helping organizations safeguard their data and comply with legal and regulatory mandates (ISO, n.d.).

The ISO 27000 family includes several key standards that collectively guide the establishment and continuous improvement of an ISMS, addressing various areas of effective information security management (ISMS.online, n.d.):

1. ISO/IEC 27001: Specifies requirements for establishing, implementing, maintaining, and improving an ISMS.
2. ISO/IEC 27002: Provides guidelines for organizational information security standards and practices.
3. ISO/IEC 27003: Offers guidance on the implementation of ISMS.
4. ISO/IEC 27004: Addresses the measurement of ISMS performance.
5. ISO/IEC 27005: Focuses on information security risk management.
6. ISO/IEC 27006: Sets requirements for bodies providing audit and certification of ISMS.

2.2 The structure of ISO/IEC 27001:2022

ISO 27001 is a framework for establishing and maintaining an ISMS, designed to protect data assets and demonstrate an organization's commitment to data security. The standard is widely recognized (ISO, n.d.) and defines the requirements for setting up, implementing, maintaining, and improving an ISMS, it serves as a guidebook for achieving information security practices (ISO, 2022). The standard involves an annual audit of a defined scope, which must be established and maintained over time. It is critical to ensure that implementing ISO/IEC 27001 does not lead to excessive bureaucracy or financial strain (ISO, 2022). When properly implemented, the standard serves as a valuable investment for SMEs, enhancing information security and yielding other organizational benefits (ISO, 2022).

Structure of the standard

ISO/IEC 27001 is structured into two primary parts: the ISMS framework (Clauses 4–10) and Annex A (Clauses 6–18), which provides a code of practice containing 14 categories of recommended information security controls and objectives. This dual structure supports organizations in addressing diverse aspects of information security management (ISO, 2022).

An ISMS integrates processes, people, and technology to establish policies and objectives aimed at keeping sensitive information safe. The CIA principles form the foundation of effective information security practices, aligning business operations with the expectations of relevant stakeholders, such as customers, while maintaining compliance with regulations like GDPR (Fortinet, n.d.; ISO, 2022).

By focusing on these components, organizations can create a flexible and efficient ISMS that balances security needs with operational efficiency, ensuring that security measures align with business objectives and stakeholder requirements (ISO, 2022).

2.3 The importance of an ISMS

An ISMS is important for any organization because it provides a structured approach to managing sensitive company information. ISO/IEC 27001:2022 outlines the key objectives of an ISMS, which are essential for protecting the CIA of information. These principles that are shown in Figure 1 ensure that information is only accessible to authorized users (confidentiality), remains unaltered and protected from unauthorized modifications (integrity), and is available to authorized users when required (availability). The CIA triad is visualized in various resources (Fortinet, n.d.; ISO, 2022; Bunker Your Risk, n.d.).

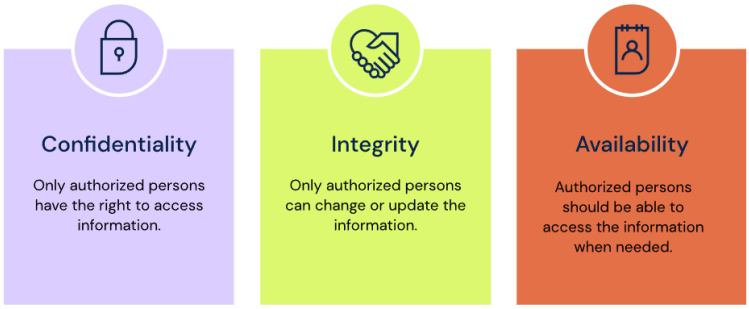

Figure 1. ISMS security objectives (6clicks, n.d.)

The benefits of implementing an ISMS are visualized in Figure 2. Many industries are subject to regulations that require businesses to implement strong information security measures, such as the GDPR and NIS2. These regulations mandate the protection of sensitive data, enhance data privacy, safeguard against cyber threats, and ensure compliance with security standards (European Union, 2016; European Union Agency for Cybersecurity [ENISA], 2024; ISO, 2022). An ISMS helps ensure compliance by protecting sensitive information from threats, reducing the risk of data breaches and financial losses. It also plays a key role in organizational resilience by continuously improving security practices to address evolving threats (ISO, 2022).

The structured approach of an ISMS clarifies roles and responsibilities, integrating security into business operations (Secfix, 2024). It also builds trust with clients and stakeholders, assuring them that their data is securely handled,

which is essential for maintaining strong business relationships and a positive reputation (ISO, 2022; UpGuard, n.d.).

An ISMS encourages a security-conscious culture by engaging employees in security practices and emphasizing their role in safeguarding information. It includes mechanisms for regular reviews and improvements to adapt to emerging threats. While security audits are necessary, they can be costly in terms of time and resources. An ISMS streamlines this process by establishing documented procedures for efficient audits (ISO, 2022; UpGuard, n.d.).

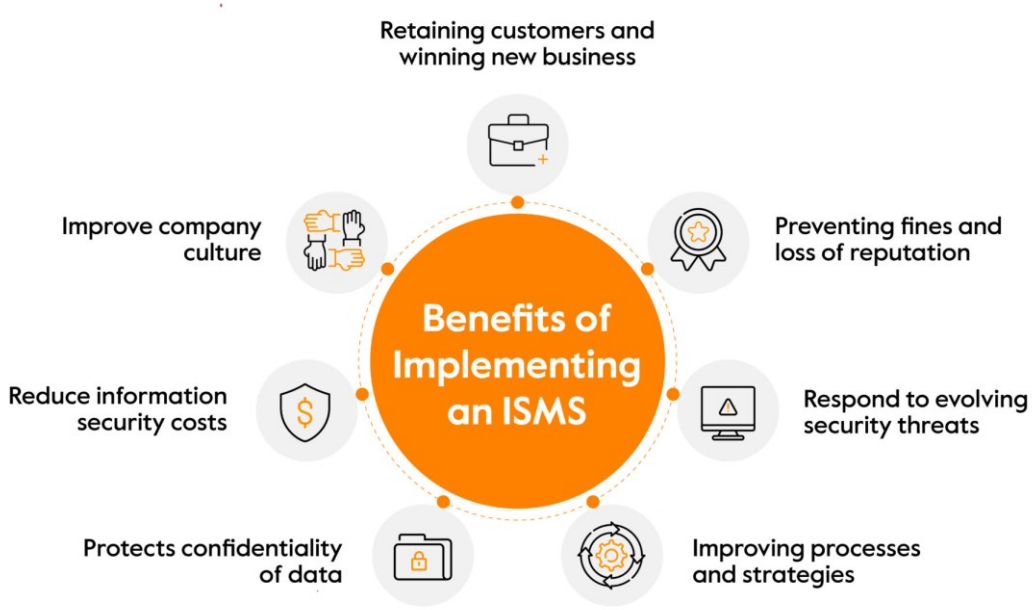

Figure 2. 7 benefits of ISMS implementation (Gracy, 2024)

Key ISMS Clauses in ISO/IEC 27001:2022

The key clauses in Table 1, related to an ISMS in ISO/IEC 27001:2022, are clauses 4 to 10. These clauses outline the essential steps for implementing and maintaining an effective ISMS that ensures the CIA of information. Below is a brief overview of each of these clauses (ISO, 2022).

Table 1. ISO 27001 Clauses 4-10

4: Context of the organization	-Identify the key stakeholders and clarify their needs and interests -Define the scope of the ISMS
5: Leadership	-Obtain commitment from leadership -Establish policies -Define roles and responsibilities
6: Planning	-Assess risks, vulnerabilities and opportunities to improve information security -Identify InfoSec objectives
7: Support	-Define and document resources for maintaining the ISMS
8: Operation	-Define risk treatment plans Implement controls
9: Performance evaluation	-Monitor, measure, and assess control effectiveness -Conduct internal audits and management reviews
10: Continuous improvement	-Identify nonconformities and corrective actions

Together these clauses help the SME to establish the ISMS (ISO, 2022).

3 Implementing ISO 27001

When implementing ISO/IEC 27001:2022, it is important to follow the framework's guidelines to align with global standards for information security. The ENISA Threat Landscape 2024 report highlights emerging cybersecurity threats such as ransomware and AI-driven attacks, emphasizing the need for organizations to adopt strong security measures. These risks make adherence to ISO 27001 even more important (ENISA, 2024).

3.1 Significance of leadership in ISMS

Effective leadership is critical to the success of an ISMS. As outlined in Subclause 5.1 of ISO/IEC 27001:2022, top management must demonstrate active leadership and commitment to the ISMS. This involves integrating information security into the organization’s governance framework and aligning it with broader business objectives. Leaders are responsible for fostering a security-conscious culture by engaging employees through communication, training, and resource allocation. Management must also support and encourage all stakeholders involved in ISMS activities to ensure its proper maintenance. By prioritizing information security, top management not only underscores its importance but also strengthens stakeholder confidence in the organization’s commitment to data protection (ISO, 2022).

3.2 Selection of team members for the project

Selecting the right team for ISO 27001 implementation is crucial to its success. The team should have diverse skills, including expertise in information security, the ISO 27001 framework, legal and regulatory requirements (such as GDPR in the EU), and project management. Team members must understand ISMS operations and possess knowledge of IT security and risk management. If internal expertise is lacking, external consultants may be needed.

Legal and regulatory compliance is key, particularly for SMEs in the EU that must adhere to GDPR. It is essential to have team members familiar with these regulations to ensure ISO 27001 certification. The project requires strong project management to stay on track, manage deadlines, and facilitate cross-departmental collaboration. IT will manage technical security controls, HR will address training and access policies, and business function representatives will ensure security measures align with operational needs. Leadership must ensure alignment with strategic goals and allocate resources.

3.3 Gap analysis

After identifying the necessary roles and defining responsibilities, the SME should evaluate the current staff's skills, experience, education, and training related to information security management (Secfix, 2024). Various risk assessment templates are available online, including those from reputable sources like ISO Docs (ISO Docs, n.d.). If a gap exists between the required and existing skills, the business must decide how to bridge that gap and take appropriate action. This process is known as a Gap Analysis. An example of a gap analysis is shown in Table 2.

This Gap evaluation assesses the SME’s current security posture by comparing existing practices with ISO 27001 requirements. Gap Analysis templates can be obtained from legitimate sources such as ISO Docs, which offer standardized templates tailored specifically for ISO 27001 certification (ISO Docs, n.d.). Organizations can also choose to create custom templates in-house. Developing a custom template provides greater flexibility, and ensures alignment with the organization’s existing processes, security practices, and specific needs, enhancing its risk management and information security framework.

Table 2. Gap analysis template example

Clause reference	Description of requirement	Current Status	Gap Description	Recommended Actions	Priority	Responsible	Target Date	Status
6.1.2	Risk assessment process	Informal process exists	Process not fully documented	Formalize process, document risk treatment	High	Security manager	2 months	In progress
7.2	Competency of personnel	No formal security training program	Employees lack formal security training	Implement regular security training program	Medium	HR Dept.	3 months	Not started

As shown in Table 2, Each row in the table could correspond to a specific ISO 27001 clause (e.g., Clauses 4–10), linking the organization's current practices to the requirements outlined in the standard. For each clause, it is helpful to summarize the requirement and assess the organization's current approach.

For instance, Clause 6.1.2 specifies the need for a formal risk assessment process to identify, evaluate, and manage risks. It's important to document whether the organization's current practices are formal, informal, or not yet in place and whether the requirement is fully, partially, or not met.

Identifying gaps between the ISO 27001 requirements and existing practices is important. For example, if a structured risk assessment process is not yet established, this should be noted. To address these gaps, recommendations can be made, such as implementing a formal risk assessment process (Secureframe, n.d.-b).

Each identified gap should be prioritized based on its potential impact on security and certification, with priority levels assigned as High, Medium, or Low. Assigning a responsible individual or team (e.g., the Information Security Manager) ensures accountability for driving the necessary improvements (ISO Docs, n.d.).

3.4 Defining the scope of the ISMS

Defining the scope is a critical step in ISO 27001 implementation. Subclause 4.5 of ISO/IEC 27001 highlights the need to define the scope, specifying which areas and assets of the organization will be protected by the ISMS. A well-defined scope ensures that resources are allocated efficiently to address key risks, supports compliance with regulatory requirements, and reinforces accountability to stakeholders (ISO, 2022).

When determining the scope, organizations should consider factors such as the organizational context, relevant interested parties, and their expectations regarding information security (ISO, 2022). An assessment of the operational infrastructure, including physical locations, technology, and business processes, helps identify which aspects should be included in the ISMS. Defining boundaries clarifies which assets, processes, and activities fall under its protection, and whether the ISMS applies to all sites or specific areas (ISO, 2022).

Aligning the scope with business objectives is essential. The SME must identify critical services, information assets, processes (e.g., HR, financial systems), and technologies (e.g., networks, servers, software) that require protection. The company should consider third-party vendors, cloud services, and outsourced IT functions that impact the ISMS, as well as relevant regulations (e.g., GDPR, NIS2) (European Union, 2016; European Union Agency for Cybersecurity, 2024).

It's important to keep the scope manageable, the company should focus on critical areas first and try to avoid over-complicating the ISMS. It is recommended to clearly document the scope, including inclusions, exclusions, and the rationale for these decisions. The SME must review and update the scope regularly to reflect changes in the business or risk environment (ISO, 2022; Secureframe, n.d.-b).

Internal and External Context in a SME

Clause 4 of ISO/IEC 27001:2022 emphasizes the importance of understanding the context in which a business operates in order to develop a reliable and strong

ISMS. Businesses must assess both internal and external factors that could impact their ISMS. The business should ensure that the system align with the organization's objectives and its information security requirements. Understanding the internal and external context is important to effectively manage information security risks and tailor the ISMS to the unique structure and operations of the organization.

Examples of internal issues. As outlined by ISO/IEC 27001:2022, include (ISO,2022):

- Organizational Structure: Gaining a clear understanding of the business hierarchy as well as the key roles and responsibilities within the business (Secfix, 2024). This includes identifying the departments and teams involved in handling sensitive information.
- Processes and systems: Conduct a review of the current processes, IT systems, and infrastructure to determine the critical areas where information security is essential.
- Company Culture: Evaluating the organization's culture in terms of security awareness, employee training, and attitudes toward data protection.
- Existing Policies and Procedures: Examining the current security measures, policies, and procedures to identify strengths and potential gaps that must be addressed.

External context refers to the factors outside an organization that can influence its ability to meet its objectives. According to ISO/IEC 27001:2022, organizations must consider internal and external issues when establishing, implementing, and maintaining their ISMS. This helps ensure that the ISMS is tailored to the specific conditions in which the organization operates.

Examples of external issues, as outlined by ISO/IEC 27001:2022, include (ISO, 2022):

- Regulatory Environment: Identifying the legal and regulatory requirements that the organization must comply with, such as data protection laws (e.g., GDPR) and industry-specific regulations.
- Market Conditions: Understanding the competitive landscape, including maintaining trust with clients and partners through strong security practices.
- Stakeholder Expectations: Considering the expectations of customers, suppliers, investors, and other stakeholders regarding data security and privacy.
- Threat Landscape: to analyze the external threats the business may face, including cyber-attacks, data breaches, and other security risks.

Example Case: Internal and External Context

A SME consulting enterprise based in Finland provides IT solutions and security consulting to clients. The enterprise relies on a mix of in-house IT systems and cloud-based services to manage sensitive client data. As the company grows, it faces the challenge of securing internal communications, intellectual property, and client information. An internal assessment of its IT infrastructure reveals potential security gaps, prompting the enterprise to align its security practices with ISO/IEC 27001 standards and ensure compliance with Finland's GDPR regulations. These efforts are crucial for both securing internal operations and maintaining client trust as the enterprise plans for ISO 27001 certification (ISO, 2022; European Union, 2016).

Externally, the enterprise must navigate pressures from government regulations, including GDPR, which mandates strict controls over personal data (European Union, 2016). It also faces increasing cybersecurity risks, such as rising cyber-attacks, which could damage client data and its reputation. To stay competitive and reassure clients, the enterprise must comply with national laws and align with

global standards like ISO 27001:2022, helping to manage information security risks and enhance stakeholder confidence.

3.4.1 Understanding the needs and expectations of interested parties.

When implementing an ISMS under ISO/IEC 27001:2022, it is important to identify and address the needs and expectations of stakeholders with an interest in the organization's information security (ISO, 2022). Meeting these expectations ensures the ISMS protects sensitive information while fulfilling regulatory, contractual, and business requirements.

Customers expect their data to be protected in accordance with privacy laws like GDPR (European Union, 2016). Failure to meet these expectations can result in reputational damage and financial losses (Federal Trade Commission, 2016). Employees expect clear security policies and effective tools to protect data, making training and awareness crucial for ISMS adherence (TrustCloud, n.d.).

Suppliers and partners, who may share or access sensitive data, also expect secure data practices. Assessing third-party security is key to avoiding supply chain vulnerabilities (ISO, 2022). Lastly, shareholders and investors expect effective management of information security risks to protect assets and ensure profitability, often seeking evidence of compliance and strong security measures (Yang, Gan, & Lau, 2019).

3.5 Developing a project plan

When developing a project plan for implementing ISO/IEC 27001:2022 and aiming for potential ISO 27001 certification, it is important for team leadership to define clear project objectives. Setting well-defined goals helps the team understand the purpose and scope of the ISO 27001 implementation, aligning the project with the organization's broader business needs and ensuring all efforts are directed towards achieving specific outcomes (ISO, 2022; Tevora, n.d.).

To effectively manage the implementation, the team should break the process down into different phases, with clear milestones for each phase. Since the implementation process can vary significantly between organizations, customizing the approach to fit the specific needs and structure of the business is crucial (Wadhwa, 2024). Milestones will make tracking of progress easier and also highlight areas where adjustments may be needed to stay on course of the implementation process (Secureframe, n.d.-a).

Implementation timeline

ISO/IEC 27001:2022, does not prescribe a specific timeline for implementation. The standard outlines the requirements for establishing, implementing, maintaining, and continually improving an ISMS, but leaves the timeline flexible to suit the specific organization's needs, context, size, and complexity.

The standard is designed to be adaptable, allowing organizations of varied sizes to implement it at their own pace (ISO, 2022). For SMEs, the implementation process duration depends on a range of different factors, these include:

- Current level of information security practices.
- Availability of resources (e.g., personnel, budget, expertise).
- Organizational complexity.
- Management buy-in and commitment.

A typical timeframe of 6-12 months is often cited by consulting enterprises and practitioners who help organizations implement the standard (Secureframe, n.d.-a; Tevora, n.d.).

Implementation phases

The implementation phases depicted in Figure 3 are an example of how the implementation process can be done as outlined by ISO 27001 (ISO, 2022).

Figure 3. ISO 27001 implementation phases (adapted from ISO, 2022)

The project overview phase involves setting the objectives for the SME and implementing the ISO/IEC 27001:2022 standards to establish, implement,

maintain, and continually improve the ISMS. This phase also includes defining the scope of the project, which means specifying the departments, systems, and processes that will be included in the ISMS. The scope may be organization-wide or limited to specific functions (e.g., IT systems, customer data). During this phase, the project leader also sets a timeline for the project. Leadership is responsible for establishing the budget, estimating costs for resources, tools, external consultants, training, certification fees, etc (ISO, 2022).

The project initiation phase includes setting key roles and responsibilities, this is further explained in Clause 5.3 of ISO/IEC 27001:2022 (ISO, 2022). This phase focuses on conducting a gap analysis, defining the scope, and gaining stakeholder buy-in.

The ISMS establishment phase involves conducting a risk assessment and developing a treatment plan, defining the Information Security policy, and establishing the procedures and controls necessary for the SME to achieve ISO 27001 certification. This phase also covers asset management and compliance with legal, regulatory, and contractual requirements (ISO, 2022).

The training and awareness phase focuses on staff training and awareness. In this phase, the SME educates employees on their roles in information security. Training topics should cover company policies, incident reporting, secure use of IT systems, phishing awareness, etc. This phase may include creating a training program and maintaining attendance records. Additionally, the training phase ensures that all ISMS-related documents are version-controlled and accessible only to authorized personnel (ISO, 2022).

ISO/IEC 27001:2022 includes ninety-three security controls in Annex A (structured into four sections). Implementing these controls in an SME may require prioritization based on risk assessment. The Annex A control includes the following categories (ISO, 2022):

1. Organizational Controls:
    - Information security roles and responsibilities.
    - Segregation of duties.
    - Contact with authorities and special interest groups.
2. People control:
    - Screening during recruitment.
    - Security awareness training.
    - Disciplinary process for security violations.
3. Physical Controls:
    - Access control to buildings.
    - Securing workstations, laptops, and mobile devices.
    - Managing visitor access.
4. Technological Controls:
    - Anti-malware protection.
    - Backup procedures.
    - Encryption.
    - Monitoring and logging.

Documentation needs to be ensured, developed, and maintained throughout the process. The ISMS documentation contains the information security policy, risk assessment methodology, statement of applicability (SOA), risk treatment plan, security operating procedures (SOP), access control policy, asset management policy, business continuity plan, and incident response plan (Wadhwa, 2024).

The internal audit phase is a critical part of the ISO/IEC 27001:2022 implementation process. During this phase, the organization conducts an internal audit to assess the ISMS's compliance with ISO 27001 requirements. This is a pre-certification audit to ensure that the ISMS documentation is complete, and

that all security controls have been effectively implemented. The organization must then document this phase by preparing an internal audit report, which details the findings and provides evidence of compliance (ISO, 2022; Tevora, n.d.).

Another essential component of this phase is the management review. Management should conduct regular reviews of the ISMS to evaluate its effectiveness and alignment with the organization's objectives. The internal audit report plays a key role here, providing management with the information needed to make informed decisions and improvements based on audit findings (Gracy, 2024).

As outlined in ISO/IEC 27001:2022, the certification audit is divided into two stages. The first stage is a document review, where an external auditor verifies that all documentation meets ISO 27001 standards. This includes ensuring that the necessary documentation is complete and accurate (ISO, 2022). The second stage is the on-site audit, during which the auditor visits the organization to verify the implementation of security controls, review evidence, and assess overall compliance with the ISMS (Wadhwa, 2024).

For the on-site audit, it is important for the organization to be well-prepared. The organization must be ready to demonstrate how the ISMS operates in practice, answer questions from the auditor, and provide relevant evidence of compliance. Once both parts of the audit are completed, the certification decision is made. If the audit is successful, the organization will be granted ISO/IEC 27001 certification, which remains valid for three years. During this period, surveillance audits are typically conducted annually to ensure continued compliance and maintain certification (Secureframe, n.d.-b).

3.6 Developing Required Documentation and Policies

Clause 7.5 outlines the need for maintaining documented information necessary for the ISMS. This includes the creation of policies, procedures, and other forms of documentation that are vital for demonstrating compliance with ISO 27001 standards.

A policy is a formal set of principles or rules that govern decisions within an organization. The information security policy should clearly reflect the organization’s management goals and outline how these objectives will be achieved. The policy should address the enterprise's commitment to safeguarding sensitive information and align with strategic business objectives (ISO, 2022).

For an SME, the establishment of a comprehensive information security policy is essential, as it forms the foundation of the ISMS and sets the tone for security practices across the organization. This policy must be communicated effectively to all employees and relevant stakeholders to ensure everyone understands their responsibilities in maintaining information security (ISO, 2022; Tevora, n.d.).

Documentation of the policy can be in various formats, such as digital, hard copy, or both, depending on the organization’s preferences (ISO, 2022). Regular reviews and updates to the policy are critical to adapting to evolving risks, regulatory changes, and emerging threats. Leadership involvement in the creation and endorsement of the policy is essential, as it highlights the organization’s commitment to information security and demonstrates its dedication to protecting valuable information assets (Secureframe, n.d.).

3.6.1 Mandatory ISMS documentation required for ISO/IEC 27001 certification.

The documentation referenced in ISO/IEC 27001 Annex A is required only if an organization deems the associated controls necessary for the implementation of its Information Security Management System (ISMS). The Annex A controls, and the documentation tied to them, are discretionary in nature and are based on the organization's risk assessment and specific needs (ISO, 2022).

The following documentation is typically required or recommended in accordance with the relevant clauses of ISO/IEC 27001:2022:

- ISMS scope (Clause 4.3, ISO, 2022)
- Information Security Policy (Clauses 5.1 and 5.2, ISO, 2022)
- Information security risk assessment procedure (Clause 6.1.2, ISO, 2022)
- Statement of Applicability (Clause 6.2.3(d), ISO, 2022)
- Information security risk treatment procedure (Clause 6.1.3, ISO, 2022)
- Information security objectives (Clause 6.2, ISO 2022)
- Personnel records (Clause 7.2, ISO 2022)
- ISMS operational information (Clause 8.1, ISO, 2022)
- Risk assessment reports (Clause 8.2, ISO, 2022)
- Risk Treatment Plan (Clause 8.3, ISO, 2022)
- Security metrics (Clause 9.1, ISO, 2022)
- ISMS internal audit program and audit reports (Clause 9.2.2, ISO, 2022)
- ISMS management review reports (Clause 9.3.3, ISO, 2022)
- Records of nonconformities and corrective actions (Clause 10.1, ISO, 2022)

To maintain ISO 27001 documentation effectively, organizations must implement structured protocols that govern the entire document lifecycle. This includes clearly assigning ownership, implementing access controls, and ensuring that documents are regularly reviewed and updated based on audit results, risk assessments, or changing business requirements. Regular reviews are essential for ensuring that the documentation stays current, accurate, and compliant with ISO 27001 standards (ISO, 2022).

Organizations should also define document retention and disposal procedures. These procedures outline how long documents should be kept and the secure methods for their disposal when outdated. This ensures sensitive information is managed and disposed of securely, mitigating the risk of breaches (Fortinet, n.d.; ISO, 2022).

To maintain consistency and efficiency in documentation, standardized templates should be used. Templates ensure that documents meet the required criteria and streamline the process of creation, making compliance and auditing easier to manage (Tevora, n.d.).

Clear communication is important for maintaining effective ISMS documentation. Using visual aids, such as flowcharts and diagrams, enhances comprehension and helps employees and stakeholders understand the policies, procedures, and controls implemented. This visual approach aids adherence to information security practices and facilitates training (ISO, 2022).

By following these protocols, organizations can create organized, compliant documentation that supports a secure and resilient information management system.

3.7 Certification audit

Before entering the ISO 27001 certification audit phase, several key factors must be addressed to ensure organizational readiness and compliance with the standard's requirements. First, top management must ensure the ISMS scope is

clearly defined, considering relevant stakeholders and their needs. The scope statement, which outlines the boundaries of the ISMS, will be reviewed by auditors to verify its alignment with the organization's business goals and regulatory obligations (ISO, 2022). A well-defined scope is essential for setting clear expectations for the audit process and aligning the ISMS with the organization's priorities.

Another critical component is the Statement of Applicability (SOA), which justifies the inclusion or exclusion of specific controls based on the organization's risk assessment. This assessment evaluates key factors such as assets, threats, and vulnerabilities. It is highly recommended that the SOA be thoroughly reviewed and maintained, as it is a crucial document in the ISO 27001 audit process (ISO, 2022). The auditors will expect to see how each control is tied to identified risks and the rationale for its inclusion or exclusion.

Preparation for the audit requires active engagement from the entire organization. Control owners will be interviewed during the audit, so departments such as IT, HR, legal, asset management, and operations must be prepared to demonstrate how their areas contribute to the effectiveness of the ISMS. Regular spot checks by top management can help ensure controls are being implemented consistently and in alignment with the SOA (ISO, 2022). This proactive approach helps identify gaps early and avoid last-minute surprises.

Top management must ensure clear communication about the certification audit process, setting expectations for all involved. Assigning control ownership within the SOA and providing control owners with access to the ISO 27001 standard will help them understand their responsibilities and how to apply the standard. This also minimizes confusion and supports consistency throughout the ISMS implementation (ISO, 2022).

Certification audits require evidence to verify that each control has been implemented effectively (ISO, 2022). This evidence typically includes documented records demonstrating the implementation and operation of

controls. Providing this evidence promptly and in a clear format helps streamline the audit process and reduces delays.

Finally, the ISMS must instill confidence that information security risks are effectively managed. Active participation during the audit walkthrough is essential to demonstrate compliance. The auditors' confidence will be influenced by the organization's ability to showcase its adherence to ISO 27001 requirements and the thoroughness of the supporting evidence provided (ISO, 2022).

3.8 Creating and Maintaining an Information Security Awareness Program

Clause 7.3 emphasizes the importance of maintaining an ongoing awareness and training program to ensure that all personnel understand their responsibilities regarding information security. Human error remains one of the leading causes of data breaches (Tessian, 2022; Breachsense, 2024), making effective training crucial for fostering a security-conscious culture and mitigating associated risks. Training should include regular sessions on potential threats, proper data handling practices, and compliance with security policies.

In addition to formal training, continuous awareness campaigns such as newsletters, posters, and digital reminders help reinforce critical security messages. The European Union Agency for Cybersecurity (ENISA) supports initiatives like European Cybersecurity Month, which encourages safe digital practices and helps raise awareness about social engineering attacks like phishing (ENISA, 2024).

For personnel in roles with elevated security responsibilities, role-specific training may be necessary to address the unique security challenges they face (Secfix, 2024). The effectiveness of the program should be regularly evaluated and updated based on participant feedback and emerging threats. Effective training programs significantly reduce the risk of human error and minimize incidents like accidental data breaches.

ISO 27001 also addresses a variety of risks, including inadequate access control, unpatched systems, third-party threats, and physical security vulnerabilities. These risks are mitigated through regular security assessments and the application of appropriate controls (ISO, 2022).

4 Case study: Cyberday as implementation tool

4.1 Context and Background of the Case Study

This case study focuses on a small IT consulting enterprise in Finland with 17 employees, which faces common challenges typical for SMEs, including limited resources, the need to quickly adapt to changing industry conditions, and managing information security with a small team. The enterprises core business is providing technical solutions to clients, including services that involve handling sensitive data.

At the beginning of its ISO 27001 implementation, the enterprise already held other certifications and was compliant with GDPR. The existing state of information security within the enterprise was relatively good but incomplete. While some essential documentation was available, other necessary documents were lacking, highlighting the need for a more structured approach to managing information security. Clients can demand ISO 27001 compliance (ISO, 2022) and thus, an ISMS was needed to meet these expectations.

4.2 Steps in the implementation

The implementation of ISO 27001 in the small IT consulting enterprise followed a structured approach, which consisted of several key phases, from planning through to potential certification. The process began with thorough planning and scoping, where the enterprise defined the boundaries of its Information Security Management System (ISMS) with the assistance of Cyberday, a platform designed to streamline ISO 27001 adoption and other cybersecurity practices (Cyberday, n.d.). The platform offers a wide range of tools to facilitate the process, including templates for policy and procedure documents, risk assessments, asset management, and ongoing compliance monitoring. Cyberday also features an Academy that provides comprehensive training videos on using the platform (Digiturvamalli, n.d.).

In the planning phase, the enterprise identified key stakeholders and assessed its existing cybersecurity risks. This phase ensured that the necessary resources, roles, and commitments were in place for a successful ISO 27001 implementation (ISO, 2022). Cyberday's tools were critical during this phase, assisting with risk assessments and providing automated reminders and tasks to ensure the organization stayed on track.

Cyberday is designed to support organizations in managing cybersecurity tasks and ensuring compliance with frameworks like ISO 27001, GDPR, and NIS2. It helps document and execute cybersecurity practices, while also offering functionality to track ongoing compliance. Additionally, Cyberday enhances employee awareness by distributing cybersecurity guidelines through collaborative platforms such as Microsoft Teams, ensuring that everyone in the organization is informed and aligned with security policies (Cyberday, n.d.).

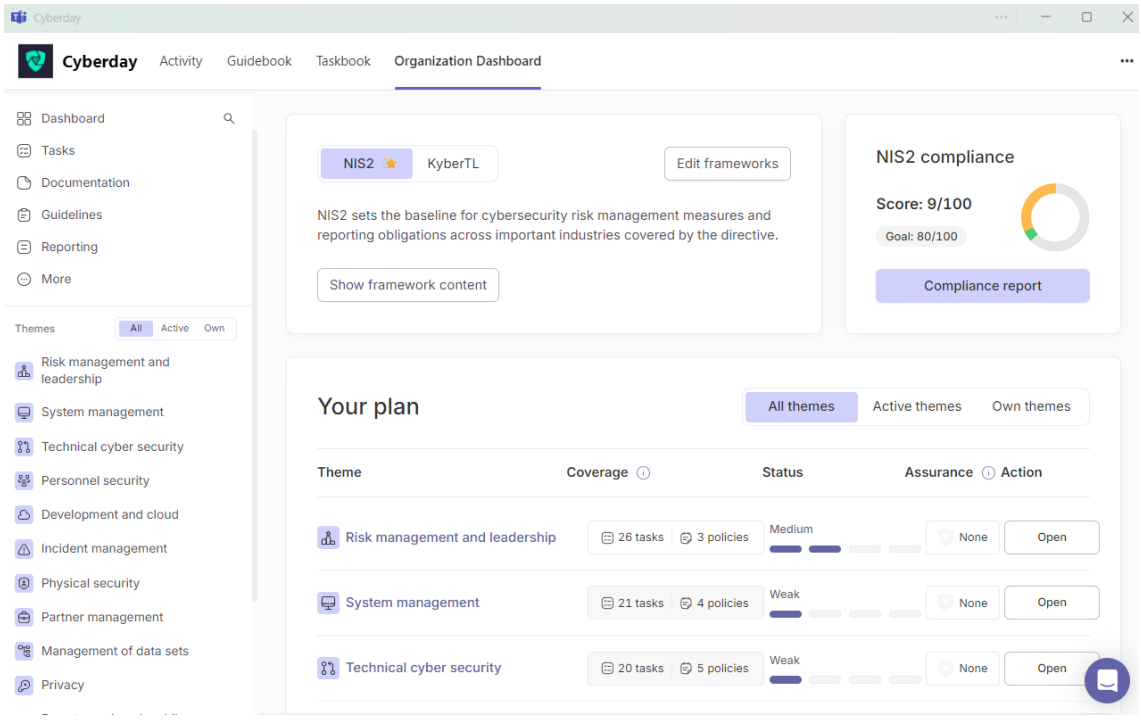

Figure 4. Cyberday layout in Microsoft Teams

As shown in Figure 4, the SME selected the frameworks it wanted to implement, choosing NIS2 (European Parliament and Council, 2022) and the Kyberturvallisuuslaki, which is still under legislation in Finland (HE 57/2024,

2024). Cyberday consistently updates its existing frameworks, such as NIS2 and ISO 27001, and introduces new ones, ensuring it stays aligned with evolving regulatory landscapes (Cyberday, n.d.). This feature makes Cyberday an excellent tool for businesses looking to adopt and manage various cybersecurity frameworks, regardless of whether certification is the end goal.

Once the desired frameworks are selected and activated, Cyberday customizes a visual structure to outline the key areas of the implementation process and assigns specific tasks. This task structure is depicted in Figure 6. In addition, Figure 5 shows the cybersecurity themes covered by Cyberday, which are directly linked to the tasks and guidelines within the platform.

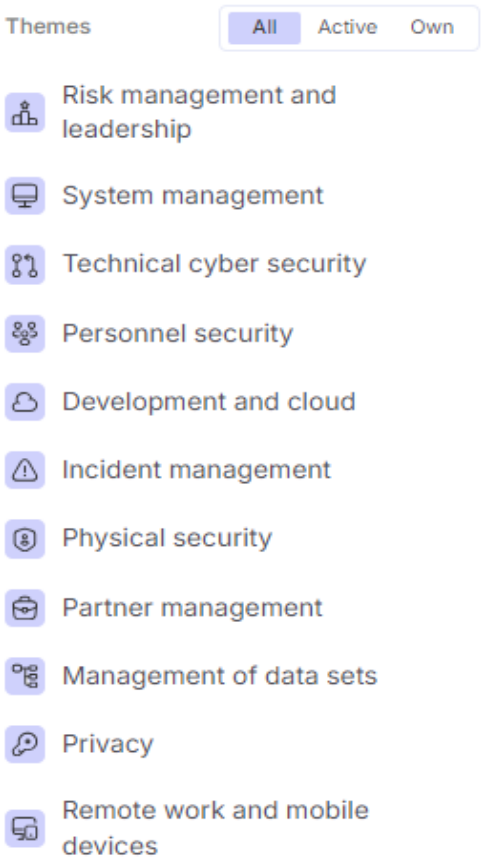

Figure 5. Cybersecurity themes in Cyberday

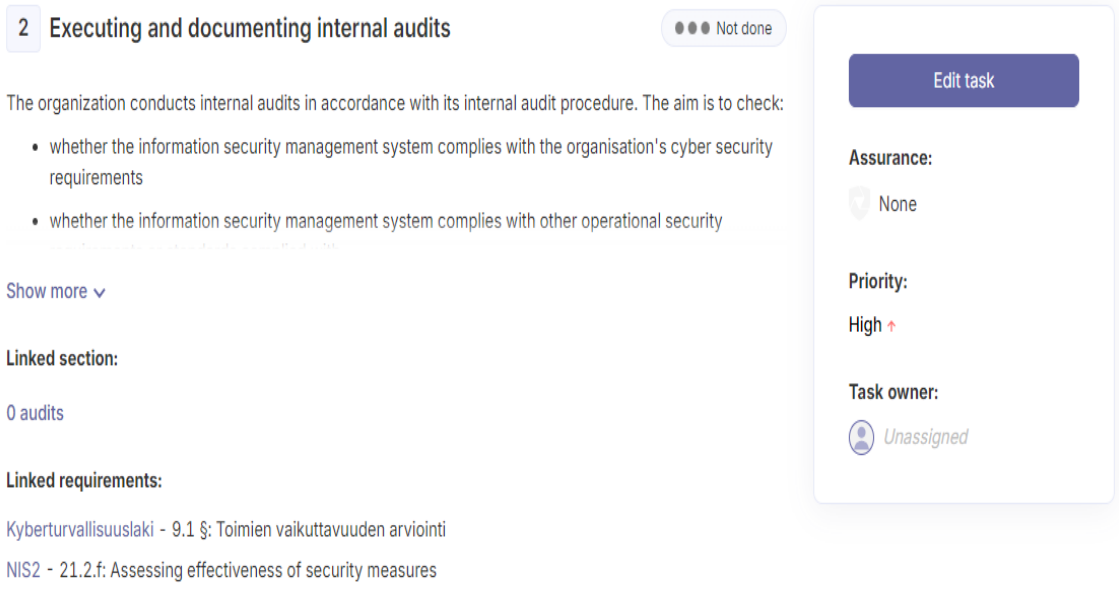

Figure 6. Cyberday task

Tasks are assigned to specific owners and evaluated based on priority and assurance levels. Once assigned, the task owner receives notifications regarding deadlines and is empowered to take timely action.

Cyberday simplifies the documentation process by providing ready-made templates for each theme and related task, which helps the SME save time (Cyberday, n.d.). The status of each task is tracked and logged, allowing the team to stay on schedule with deadlines, as shown in Figure 7. Additionally, the activity tab alerts the team when a task is approaching its due date, helping to ensure nothing is overlooked.

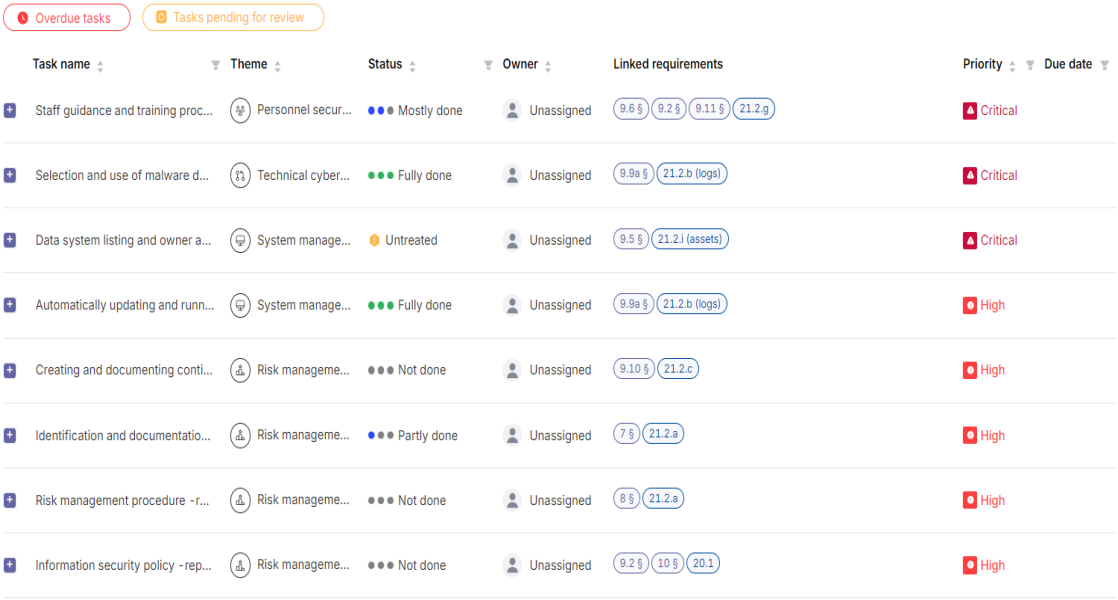

Figure 7. Cyberday task log

The project documentation can be created and stored directly within Cyberday, further streamlining the implementation process. As the project progresses, the team can collect all relevant documentation and data on Cyberday, which can then be used to generate a compliance report, ensuring the organization stays on track with ISO 27001 requirements (Cyberday, n.d.).

Phases of Implementation

The different implementation phases of ISO 27001 required majority of the work in the SME, the implementation phases are visualized in Figure 8.

1. Initial Assessment and Gap Analysis: The first step involved conducting an initial assessment by a top management individual or individuals to understand the enterprises' current information security posture. Project team members were selected from different areas within the SME and invited through e-mail to Cyberday. This phase included a gap analysis to identify areas that did not align with ISO 27001 requirements. With the help of Cyberday and the ISO 27001 standard, the team was able to visualize the necessary tasks and plan the next steps in the process with the help of Cyberday. The enterprise also reviewed its existing documentation, confirming that some elements were in place, such as GDPR compliance and previous ISO 9001 certifications.
2. Designing the ISMS: In this phase, the enterprise designed its ISMS with the help of Cyberday, based on the results of the initial gap analysis. Documentation was added to Cyberday, which made it easier to organize and navigate, since all documentation related to the implementation project was on one platform. Key components included defining policies, procedures, and controls that would address identified risks and meet the specific requirements of ISO 27001. A SOA was developed on Cyberday to justify the inclusion or exclusion of certain controls, based on the enterprise risk assessment. All necessary documentation was tagged and put into Cyberday to check the implementation tasks.

3. Implementation of Controls: With the design in place, the enterprise proceeded to implement the necessary security controls. This included the development of specific security policies, setting access controls, and implementing risk mitigation strategies. Tools like Cyberday were utilized to help automate and organize the management of security controls and track progress. Cyberday provided real-time monitoring and reporting capabilities, enabling the enterprise to stay on top of compliance efforts and address any potential issues in a timely manner (Cyberday, n.d.).
4. Internal Audits and Continuous Monitoring: During the implementation phase, the enterprise conducted internal audits to ensure that the ISMS was operating effectively and meeting ISO 27001 standards. This step also involved ongoing monitoring to identify and address any gaps or weaknesses in the system.

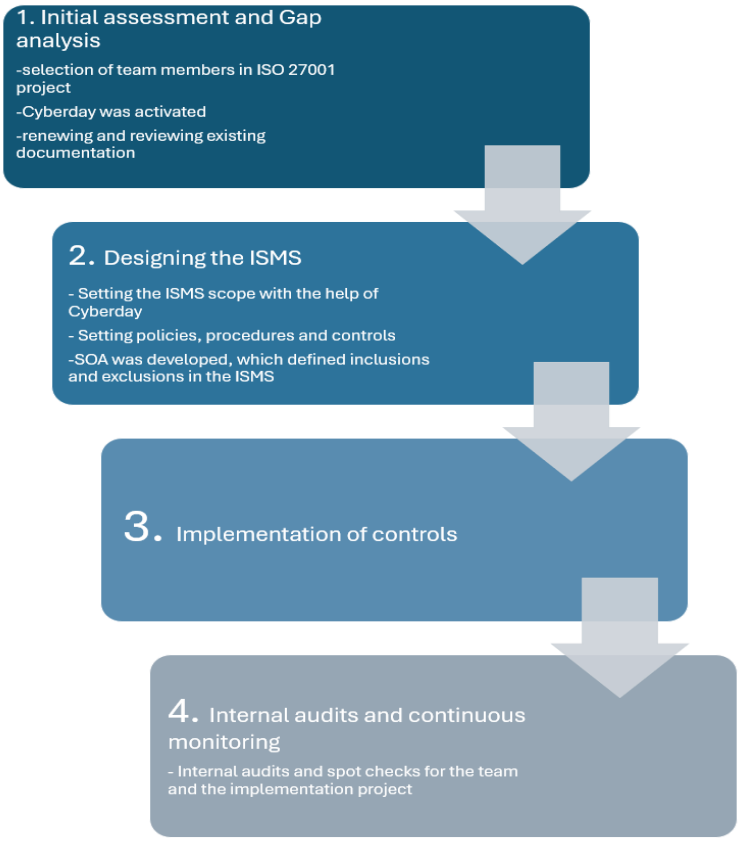

Figure 8. Implementation phases

Throughout this implementation process, a tool like Cyberday played a crucial role in tracking progress, managing risks, and ensuring that all necessary documentation and controls were in place and stored. The use of such a tool helped streamline the implementation process, ensuring that the enterprise remained on track to meet the ISO 27001 certification requirements (Cyberday, n.d.).

4.3 Challenges during implementation

When implementing ISO 27001 in a SME, several challenges can arise. An example of such challenges could be resource constraints, including limited personnel, budget, or time (Chidukwani, Zander, & Koutsakis, 2022). In the case of the SME in this study, a smaller team compared to larger organizations made it difficult to allocate dedicated resources for essential tasks like risk assessments, policy development, and internal audits. Specific challenges faced by the SME included:

- Lack of Expertise: SMEs may lack in-house information security experts, leading to a reliance on external consultants, which can increase costs (Chidukwani, Zander, & Koutsakis, 2022).
- Cultural Resistance: Employees might resist new security policies or fail to grasp their importance, creating friction during implementation (Whatfix., n.d.).
- Complexity of Documentation: Managing and maintaining the extensive documentation required for ISO 27001 can overwhelm small teams (ISO, 2022).
- Budget Constraints: Costs for hiring consultants, conducting gap analyses, and preparing for certification audits can strain an SME's financial resources (Chidukwani, Zander, & Koutsakis, 2022).
- Time Pressures: Balancing implementation efforts with day-to-day operations can be a challenge for SMEs, requiring careful prioritization (ISO, 2022).

These challenges underscore the importance of careful planning, utilizing tools like automated platforms (e.g., Cyberday), and fostering strong organizational buy-in for successful ISO 27001 implementation (Cyberday, n.d.).

5 Conclusion

The thesis has explored the process of ISO 27001 implementation within a small IT consulting enterprise, analyzing the challenges, strategies, and tools involved. Through a case study, we examined how the enterprise addressed the complexities of establishing an ISMS, achieving compliance with ISO 27001 standards, and meeting the specific needs of an SME.

By utilizing tools such as Cyberday, the enterprise managed to organize the complex implementation process, benefiting from a structured framework for managing cybersecurity tasks, maintaining documentation, and tracking progress. These features significantly helped efficiency and organization, enabling the enterprise to fulfill ISO 27001 requirements while strengthening its overall information security and risk management practices.

Notable progress was achieved in aligning the enterprise practices with ISO 27001, particularly through Cyberday's functionalities, such as templates for policy creation, risk management tools, and automated reminders. These capabilities were instrumental in conducting gap analyses, implementing security controls, and staying on track with project objectives. As a result, the enterprise successfully established the necessary policies, procedures, and controls, conducted internal audits, and demonstrated a commitment to continuous improvement. However, the certification audit remains a critical final step.

This research underscores the importance of thorough planning, structured approaches, and the integration of automation tools in the ISO 27001 implementation process, particularly for SMEs. The case study demonstrates that even small organizations with limited resources can successfully develop an ISMS that meets global standards, enhances security, and fosters business sustainability.

The findings contribute to the broader understanding of the practical challenges SMEs encounter in pursuing ISO 27001 certification, as well as the pivotal role of automation tools like Cyberday in simplifying and accelerating the process.

Future research could explore the long-term impacts of ISO 27001 certification on SME resilience to cyber threats, client relationships, and organizational growth. Ultimately, this case study illustrates that with effective planning and the right tools, SMEs can establish robust information security systems that not only ensure compliance but also support strategic objectives and drive sustainable development.

References

6clicks. (n.d.). What are the 3 ISMS security objectives? 6clicks. Retrieved September 12, 2024, from https://www.6clicks.com/resources/answers/what-are-the-3-isms-security-objectives

Breachsense. (2024, April 19). How human error causes data breaches. Breachsense. Retrieved October 20, 2024, from https://www.breachsense.com/blog/data-breach-human-error/

Bunker Your Risk. (n.d.). Understanding cybersecurity. Retrieved December 15, 2024, from https://www.bunkeryourrisk.com/understanding-cybersecurity/

Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A survey on the cyber security of small-to-medium businesses: Challenges, research focus and recommendations. IEEE Access, 10, 1–1. https://doi.org/10.1109/ACCESS.2022.3197899

Cyberday. (n.d.). Cyberday. Retrieved October 25, 2024, from https://www.cyberday.ai/

Digiturvamalli. (n.d.). Digiturvamalli Akatemia [Cyberday Academy]. Retrieved October 25, 2024, from https://www.digiturvamalli.fi/akatemia

European Data Protection Board. (n.d.). Data protection benefits for you. European Data Protection Board. Retrieved October 13, 2024, from https://www.edpb.europa.eu/sme-data-protection-guide/data-protection-benefits-for-you_en

European Parliament and Council. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union. Retrieved September 29, 2024, from https://eur-lex.europa.eu/eli/dir/2022/2555/oj?locale=fi

European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). EUR-Lex. Retrieved October 15, 2024, from https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A32016R0679

European Union Agency for Cybersecurity (ENISA). (2024). ENISA threat landscape 2024. European Union Agency for Cybersecurity. Retrieved November 23, from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

European Union Agency for Cybersecurity. (n.d.). Cybersecurity awareness campaigns. ENISA. Retrieved September 14, 2024, from https://www.enisa.europa.eu/topics/cybersecurity-education/awareness-campaigns

Federal Trade Commission. (2016). Protecting personal information: A guide for business. Retrieved October 5, 2024, from https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business

Fortinet. (n.d.). What is the CIA triad and why is it important? Fortinet. Retrieved November 24, 2024, from https://www.fortinet.com/resources/cyberglossary/cia-triad

HE 57/2024. (2024). Hallituksen esitys eduskunnalle kyberturvallisuuslain muuttamisesta ja eräiksi siihen liittyviksi laeiksi (HE 57/2024) [Government proposal to amend the Cybersecurity Act and related laws]. Finlex. Retrieved November 1, 2024, from https://www.finlex.fi/fi/esitykset/he/2024/20240057

Gracy, M. (2024, October 10). 7 benefits of ISMS implementation. Sprinto. Retrieved November 2, 2024, from https://sprinto.com/blog/benefits-of-implementing-isms/

International Organization for Standardization. (n.d.). ISO/IEC 27000 family — Information security management systems. Retrieved October 27, 2024, from https://www.iso.org/standard/iso-iec-27000-family

International Organization for Standardization. (2022). ISO/IEC 27001:2022—Information security management systems—Requirements. Retrieved August 29, 2024, from https://www.iso.org/standard/70242.html

ISMS.online. (n.d.). ISO 27000 standards and frameworks. Retrieved December 1, 2024, from https://www.isms.online/iso-27000/

ISO Docs. (n.d.). Gap analysis template. ISO Docs. Retrieved October 8, 2024, from https://iso-docs.com/products/gap-analysis-template

Secfix. (2024, October 9). Key roles and responsibilities in ISO 27001 implementation. Secfix. Retrieved September 21, 2024, from https://www.secfix.com/post/key-roles-and-responsibilities-in-iso-27001-implementation

Secureframe. (n.d.-a). ISO 27001 certification timeline: How long does it take? Secureframe. Retrieved November 10, 2024, from https://secureframe.com/hub/iso-27001/certification-timeline

Secureframe. (n.d.-b). ISO 27001 risk assessment. Secureframe. Retrieved November 25, 2024, from https://secureframe.com/hub/iso-27001/risk-assessment

Tessian. (2022). Psychology of human error [Tessian report]. Retrieved September 19, 2024, from https://f.hubspotusercontent20.net/hubfs/1670277/%5BCollateral%5D%20Tessian-Research-Reports/%5BTessian%20Research%5D%20Psychology%20of%20Human%20Error%202022.pdf

Tevora. (n.d.). ISO 27001: Key considerations, steps, and transition. Tevora. Retrieved November 24, 2024, from https://www.tevora.com/blog/iso-27001-key-considerations-steps-and-transition/

TrustCloud. (n.d.). Information security policies: The crucial role in achieving regulatory compliance. Retrieved December 15, 2024, from https://community.trustcloud.ai/docs/grc-launchpad/grc-101/governance/information-security-policies-the-crucial-role-in-achieving-regulatory-compliance/

University of Queensland. (n.d.). Why is information protection important? University of Queensland. Retrieved November 1, 2024, from https://data.uq.edu.au/data-and-information-essentials/why-information-protection-important

UpGuard. (n.d.). What is information security? UpGuard. Retrieved September 15, 2024, from https://upguard.com/blog/information-security

Wadhwa, P. (2024, October 2). ISO 27001 mandatory documents: A comprehensive list. Sprinto. Retrieved October 30, 2024, from https://sprinto.com/blog/iso-27001-mandatory-documents/

Whatfix. (n.d.). Top 12 causes of resistance to change in organizations. Retrieved December 15, 2024, from https://whatfix.com/blog/causes-of-resistance-to-change/

Yang, L., Gan, H., & Lau, L. (2019). Investors' perceptions of the cybersecurity risk management reporting framework. International Journal of Accounting and Information Management, 28(1), 1–15. Retrieved from https://www.researchgate.net/publication/336699616_Investors'_Perceptions_of_the_Cybersecurity_Risk_Management_Reporting_Framework