Bachelor’s thesis

Degree program: Information and Communications Technology, Data Networks and Cybersecurity.

Completion year of the thesis: 2024

Sebastian Peltonen

ISO27001 Implementation Handbook

TURKU AMK
TURKU UNIVERSITY OF
APPLIED SCIENCES

Bachelor’s Thesis | Abstract

Turku University of Applied Sciences

Degree program: Information and Communications Technology, Data Networks, and Cybersecurity.

Completion year of the thesis: 2024 | Total number of pages: 64

Author: Sebastian Peltonen

ISO27000 Implementation Handbook

This thesis aims to provide a comprehensive guide on planning and obtaining certification to the ISO 27000 standard. It begins with an overview of the primary standards essential for certification, emphasizing ISO 27001 as the cornerstone due to its central role in information security management.

Section 2 delves into the intricacies of planning the certification process, offering a detailed breakdown into four phases. The four phases will take you from start to finish of an audit process. This approach furnishes readers with a thorough comprehension of the entire process and the scale of an ISO 27000 audit.

Section 3 conducts a thorough exploration of the ISO 27001 audit and certification process, delineating the requisite requirements and best practices essential for achieving the standard. Each section is accompanied by a concise fictional case study, illustrating the operational procedures of a fictional organization. This addition aims to foster relatability and facilitate a comparative understanding, particularly for individuals new to the ISO 27001 audit process.

In conclusion, the thesis endeavors to furnish readers with a comprehensive understanding of the audit process and its requisites, emphasizing the holistic mindset necessary for a successful audit process.

Keywords:

ISO27000, information security, cybersecurity, handbook, ISMS.

Content

Pictures:

List of abbreviations or symbols:

Abbreviation	Explanation of abbreviation
BYOD	Bring Your Own Device
IPR	Intellectual property rights
ISMS	Information Security Management System
ISO	International Organization for Standardization
NDA	Non-Disclosure Agreements
PII	Personally Identifiable Information

Introduction

The ISO 27000 series refers to a set of standards developed by the International Organization for Standardization (shortened to ISO), that focuses on information security management. These standards provide a framework for organizations to establish, implement, maintain, and continually improve an Information Security Management System, shortened to ISMS. The framework helps the cyber security expert verify his or her practice within a cyber security department in depth and gain an understanding about their own cyber security methods and data.

The core standard within the ISO 27000 series, which is usually followed within implementation is the ISO 27001 standard. It lays out the core requirements for any cyber security department or service within an organization. This includes assessing risks, implementing security controls, and setting up processes to manage and mitigate information security risks effectively.

There have been several versions of the ISO 27001 standard since its inception, with each version aiming to enhance and refine the requirements for information security management. The most recent version is ISO 27001:2022, which replaced the previous version, ISO 27001:2013. The 2022 version brought updates and improvements to better address the evolving landscape of information security threats, continuous improvement in new ways, and technological advancements.

The central aims of this text are to offer thorough insights into the ISO27000 standard and its significance in audit protocols, aiming to enhance your understanding of the audit process from start to completion. Simultaneously, it delves deeply into the ISO27001 standard, which serves as the primary benchmark for certification comparison.

When delving into the ISO 27000 series, emphasizing ISO 27001 is essential as it serves as the cornerstone for implementing a successful ISMS. This standard outlines the prerequisites for organizations to create and uphold a resilient system guaranteeing the confidentiality, integrity, and availability of information assets, consequently mitigating risks associated with breaches in information security. By prioritizing ISO 27001, we will explore the precise requirements, controls, and methodologies outlined in the standard, facilitating your organization's ability to adopt a thorough and customized strategy for proficiently managing information security risks.

The content within this thesis draws heavily from the referenced literature listed below in the reference section; however, it is essential to note that explicit citations from specific sources have not been consistently utilized throughout.

In sections 2.1 through 2.9, the content was influenced by insights from "ISO/IEC 27001:2022: An Introduction to Information Security and the ISMS Standard" authored by Steve G. Watkins.

In section 2.10, which delves into the topic of "Planning the ISO27000 certification" and draws extensively from the insights provided in "Building an ISO 27001-Compliant Cybersecurity Program: Getting Started with Marc Menninger." It's crucial to mention that the case studies presented herein are entirely fictitious and not grounded in any material.

In Section 3 of this work, the content is rooted in a diverse array of reputable sources within the field of information security management. These include "Information Security Risk Management for ISO 27001/ISO 27002" authored by Steve G. Watkins in 2019, "ISO/IEC 27001:2022: An Introduction to Information Security and the ISMS Standard" by Steve G. Watkins, released in 2022, "ISO/IEC 27001:2022 (ISMS) Awareness Training" provided by Operational Excellence Consulting in January 22, 2023, "ISO 27000 Series, The Ultimate Step-By-Step Guide" by Gerardus Blokdyk, published on August 19, 2021, and "Business Case for an Information Security Management System (ISMS) based on the ISO/IEC 27000 Family of Standards Version 5 2023" by ISO27k Forum.

2. Cybersecurity with IS027000

The ISO 27000 series is a family of standards that provide a framework for Information Security Management Systems. There are multiple different series in this family of standards, the most commonly used are ISO 27000 ISO 27001, ISO 27002, ISO 27003, ISO 27004, ISO 27005, ISO 27006, and ISO 27007. In total, there are 63 different series in the ISO27000 family. These standards are all designed to help organizations establish, implement, maintain, and continually improve their information security practices. ISO27001 is by far the most popular to compare your organization to for its vast and compelling security requirements.

Standards in the IS027000 series:

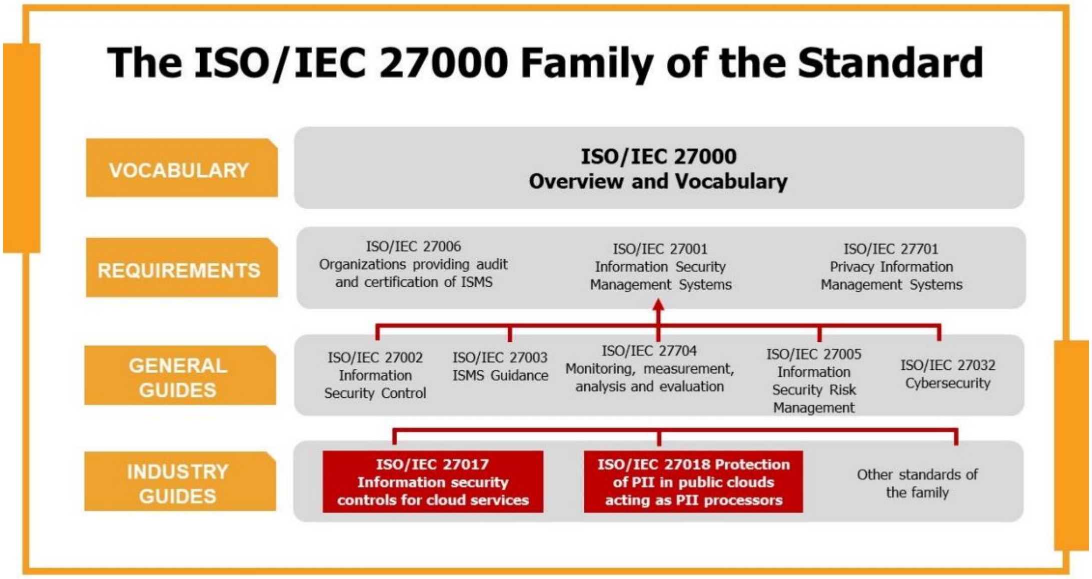

The ISO/IEC 27000 Family of the Standard
VOCABULARY
ISO/IEC 27000 Overview and Vocabulary
REQUIREMENTS
ISO/IEC 27006 Organizations providing audit and certification of ISMS
ISO/IEC 27001 Information Security Management Systems
ISO/IEC 27701 Privacy Information Management Systems
GENERAL GUIDES
ISO/IEC 27002 Information Security Control
ISO/IEC 27003 ISMS Guidance
ISO/IEC 27704 Monitoring, measurement, analysis and evaluation
ISO/IEC 27005 Information Security Risk Management
ISO/IEC 27032 Cybersecurity
INDUSTRY GUIDES
ISO/IEC 27017 Information security controls for cloud services
ISO/IEC 27018 Protection of PII in public clouds acting as PII processors
Other standards of the family

Figure 1 - Picture 1 - Picture provided by CFE CERTIFICATION February 16, 2021.

2.1 ISO 27000 - Information Security Management Systems Overview and Vocabulary:

ISO 27000 provides an overview of information security management systems and establishes common terminology used throughout the series. Serves as an introductory and foundational document for the entire series.

2.2 ISO 27001 - Information Security Management System Requirements:

The central standard outlines the requirements for establishing, implementing, maintaining, and continually improving an ISMS. It provides a risk-based approach to managing information security.

ISO 27001 stands out as one of the most widely adopted standards for information security. This is the standard that our fictional case study will dive into in section 3 and create a realistic scenario. ISO27001 is the standard that contains everything necessary for a successful cybersecurity operation. Other standards are still worth checking because they can have a deeper dive into certain sectors of cybersecurity within an organization.

2.3 ISO 27002 - Code of Practice for Information Security Controls:

ISO 27002 complements ISO 27001 by offering a set of best practices and guidelines for implementing the security controls specified in ISO 27001. It covers various aspects of information security management, helping organizations tailor their controls to their specific needs.

2.4 ISO 27003 - Information Security Management System Implementation Guidance:

ISO 27003 provides detailed guidance on the implementation of an ISMS based on the requirements specified in ISO 27001. It assists organizations in effectively planning, implementing, and documenting their information security management systems.

2.5 ISO 27004 - Information Security Management Measurement:

ISO 27004 focuses on measurement and metrics related to information security. It provides guidance on monitoring, measuring, analyzing, and evaluating the performance of an ISMS, helping organizations assess the effectiveness of their security controls.

2.6 ISO 27005 - Information Security Risk Management

ISO 27005 provides a framework for information security risk management. It assists organizations in identifying, assessing, and managing risks effectively within the context of their ISMS.

2.7 ISO 27006 - Requirements for Bodies Providing Audit and Certification of Information Security Management Systems:

2.8 ISO 27006 specifies the requirements for organizations providing audit and certification of information security management systems. It ensures consistency and reliability in the certification process.

2.9 ISO 27007 - Guidelines for Information Security Management Systems Auditing:

ISO 27007 provides guidelines for auditing information security management systems. It assists auditors in planning, conducting, and reporting on ISMS audits, ensuring the effectiveness of the security controls.

2.10 Planning the ISO27000 certification:

Before proceeding to the next chapter, it's pertinent to acknowledge the utilization of external resources within this section. Specifically, in section 2.10, which explores the intricacies of "Planning the ISO27000 certification," the content heavily relies on the expertise and insights presented in "Building an ISO 27001-Compliant Cybersecurity Program: Getting Started with Marc Menninger."

Phase 1: Form a team and create a plan for implementation.

Define the goals and needs of the organization's information security and try to outline what are the most important factors. Remember to set out clear start objectives when starting the project, otherwise it could become extremely overwhelming. The audit process is lengthy and demanding, requiring a thorough comparison of your organization's methods and security measures against the established ISO27000 standards, typically starting with ISO27001.

Establishing a team is typically crucial for facilitating workflow efficiency, ensuring clarity regarding roles and responsibilities within the audit process. Dividing tasks and prioritizing specific sections is advisable to optimize productivity. Getting crucial information out to everyone in charge of the project is highly important, for security and workflow reasons. Members in legal, security, IT, HR, and finance all need to be up to date on the matter and ready to answer questions and provide evidence if needed for the internal audit and upcoming certification audit. This especially concerns heads of departments, project managers, directors, developers, etc. Bring together individuals who will have the primary responsibility for planning and executing ISO 27001 compliance.

Phase 2: Define the scope and establish the baseline for the Information Security Management System.

Specify the scope of your organization's operations by defining the services or system's security needs. Look into all of the main series within the ISO 27000 family and define your scope with that information. Following this, conduct an internal audit to establish a baseline of your organization's current status to the ISO requirements. Establishing a baseline involves determining your current starting point before initiating the process, which includes identifying any existing known issues or deficiencies. Prioritize identified gaps based on factors such as effort, impact, and cost. This strategic prioritization will give a roadmap for the next steps in your ISO implementation, and it will also highlight potential smaller projects that could appear during the audit.

Making the internal audit and defining the scope of the project will help you budget the project correctly. Allocating staff and funds will now be clearer on how much work there is to be done. Identify the human, technical, and financial resources required for the project. This includes personnel for project management, training, and implementation, as well as technology and tools needed to enhance information security. Remember to consider the need for external consultants or experts who specialize in ISO 27000 implementation. Budget for their services, especially if the organization lacks in-house expertise.

Having this completed before phase 3 is imperative to have a successful, comprehensible, and cost-effective audit. ISO27000 audits can quickly become out of budget or not time efficient.

Phase 3: Deploy the Information Security Management System Requirements and specify and execute a risk management procedure.

In Phase 1 the plan was made, and the scope was defined in Phase 2, here in Phase 3 you only need to follow the plan and readjust, when necessary, according to the scope. Implement all gaps that were found in the internal audit, and accordingly to the ISO requirements. If need be, creating a steering committee could help ensure the project's success. A steering committee will help with strategic direction, resource allocation, risk management, monitoring progress, and overall decision-making. In larger corporations, this is not a recommendation and more of a must-have. On smaller scale businesses this is still highly useful but could be highly costly and not enough workforce to be allocated to a steering committee. It means a consultant or other outside labor would be needed to be hired and help oversee the project. Having a consultant is a great asset when in phase 3 but remember to have taken this into account in phase 1 when planning and making the budget in phase 2 for the ISO 27000 project.

At the back of creating the steering committee, it would be recommended to draft information security policies and run them through the steering committee or consultant whichever procedure is in use. These policies would, for example, Information Classification, Access Control, Data Encryption, Acceptable Use Policy, Incident Response, Physical Security, and Security Awareness Training policy. Encourage feedback and ensure that the policies align with the organization's objectives and risk assessment. Upon approval, distribute the policies to all relevant personnel and implement a communication plan to ensure awareness and understanding across the organization.

Section 3 will comprehensively address all the policies mentioned above, providing a detailed specification within the context of ISO 27000 requirements for enhanced clarity.

For the risk management, outline the approach your organization takes to recognize, prioritize, and address risks. This requires expertise from your organization to make proper and defined risk assessments within the service. The risk assessment will include constructing the risk register by listing the risks identified in earlier stages. Subsequently, develop a risk treatment plan outlining strategies to address and mitigate these risks.

Start the process with asset identification and by listing all the known risks and vulnerabilities. Everyone involved needs to be educated on the risks and vulnerabilities and increase awareness within the organization of them. This is best made in hand with vulnerability assessment, likelihood assessment, threat and impact analysis, and risk determination. Carrying out this will help you be more aware of the situation at hand and help with the prioritization of tasks.

Vulnerability assessment identifies and assesses vulnerabilities in the organization's infrastructure, systems, and processes. This includes potential weaknesses that could be exploited by threats. This could be, for example, a lack of awareness within the organization of cyber threats.

The threat and impact analysis will identify potential threats and adversaries that could exploit vulnerabilities in the organization's cybersecurity posture. This may include malicious actors, natural disasters, or other events that could compromise security. Providing at the same time the potential impact of a successful cyber-attack, considering the confidentiality, integrity, and availability of critical assets.

Risk determination will on the other hand combine the likelihood and impact assessments to determine the overall risk level for each identified threat-vulnerability pair. This helps prioritize risks based on their potential severity. This will be crucial to achieve, for future risk mitigation and monitoring.

The last parts would be communication and documentation. Maintain thorough documentation of the entire risk assessment process, including findings, analyses, and mitigation strategies. This documentation is crucial for compliance, audits, and continuous improvement. Without documentation, the ISO27000 certification is impossible to achieve.

Communication needs to ensure effective communication of risk findings and mitigation strategies to relevant stakeholders and employees within the organization. This promotes awareness and encourages a proactive approach to cybersecurity.

A well-executed risk assessment in cybersecurity provides organizations with insights to make informed decisions about resource allocation, security investments, and the overall improvement of their security posture. Simultaneously, the risk assessment encapsulates the essence of the ISO27000 series, effectively managing information security, and aligning with the proactive approach to address and mitigate prevalent cybersecurity threats through the establishment of comprehensive controls, protocols, and best practices.

Phase 4: Assess, oversee, and evaluate the Information Security Management System.

Establish and utilize the required systems and resources for supervising the ISMS. This may involve incorporating security metric dashboards, conducting routine security assessments, implementing log monitoring systems, and arranging third-party evaluations of your ISMS.

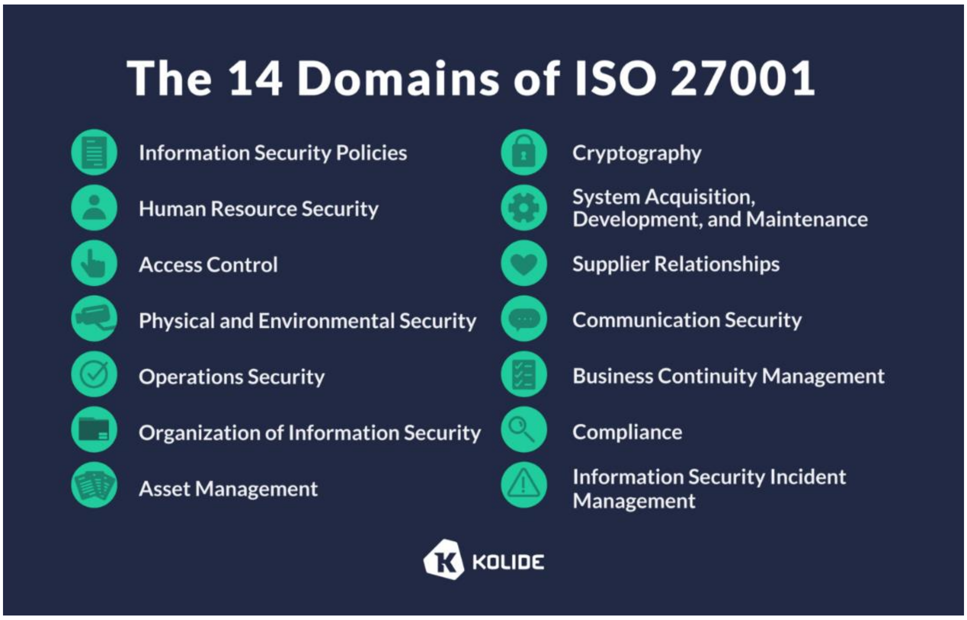
Overseeing is crucial with the need for constant improvement of the ISMS. Constant improvement in an ISMS is crucial to keep pace with changing security landscapes, maintain compliance, address weaknesses, optimize resources, enhance resilience, and demonstrate an ongoing commitment to information security.

Creating protocols and documentation on how to monitor cyber security within the organization is vital. It helps with onboarding new employees, training, and awareness for all employees involved. Defined and documented protocols will ensure ISO27000 standard certification, if it is not documented it will not pass the standard.

The overseeing, protocols, and evaluations made apply the insights gathered from these evaluations to progressively refine and enhance the state of your ISMS.

3. Components of the ISO27001 package

Starting now with a systematic examination of the ISO 27001 series requirements, our objective is to dissect each section methodically, delving into practical applications within short-described scenarios. Each primary section will feature a short case study aimed at enhancing your comprehension of the section's content and making it more applicable in practice. Throughout this examination, we will use hypothetical but realistic cases to show how organizations can address the challenges presented by contemporary information security landscapes. By breaking down the ISO 27001 standard, aiming to provide concrete insights and actionable strategies for strengthening Information Security Management Systems.



The 14 Domains of ISO 27001

- Information Security Policies
- Human Resource Security
- Access Control
- Physical and Environmental Security
- Operations Security
- Organization of Information Security
- Asset Management
- Cryptography
- System Acquisition, Development, and Maintenance
- Supplier Relationships
- Communication Security
- Business Continuity Management
- Compliance
- Information Security Incident Management

KOLIDE

Figure 2 - Picture 2 - Picture provided by KOLIDE, July 22, 2022, in the deep dive written by Elaine Atwell.

3.1 Background of the fictional organization:

The fictional organization X is a large-sized IT company specializing in software development, has recently recognized the importance of information security due to increased cyber threats in their industry. Despite having implemented some security measures in the past, they acknowledge that their practices have become outdated over time, leaving them vulnerable to potential breaches. In response, the organization has decided to undergo an ISO27001 audit to assess their current security posture and identify areas for improvement. They understand that achieving ISO27001 certification will not only enhance their cybersecurity resilience but also improve their credibility with clients and stakeholders.

3.2 Case in information security policies.

The information security policies were last updated four years ago, and organization X recognized the need for a thorough review to address emerging cyber threats and changes in business processes.

3.2.1 Policies for information security.

The existing information security policies were last updated four years ago, and since then, the technological landscape and cybersecurity threats have evolved significantly. The security policy might not need to be rewritten completely, but additions and a review of the policy must be conducted.

Elements that are required to be defined within a security policy:

- Business strategy. The security policy must integrate with the strategic objectives of the organization, ensuring a relationship between information security and its business goals.
- Countries and regions´ legislation, regulations, and contractual agreements their requirements to be followed and promised to abide by.
- An overview of the present and anticipated threat landscape in the realm of information security. This needs to contain a definition of information security for the organization, a framework to ensure security objectives

  are up to standard, principles that guide the activities in the organization, and responsibilities within information security.
- Provide a commitment to all relevant information security mandates and dedication to continuously improving information security.

Review of the policies for information security.

A yearly review at least is necessary to provide the ISO27001 certification. Evidence of the reviews or scheduling needs to be provided for the audit.

Recommendation would be to have a team look through the security policy which in place, and check if it still contains everything needed to pass the ISO27001 requirements and the businesses requirements to mitigate risks associated with cyber threats, unauthorized access, and data breaches, while fostering a culture of information security awareness and responsibility. This would update the security policy and serve as evidence for the ISO27001 audit, if documented comprehensively. The document needs to define the review process, findings, changes, and timestamps.

3.3 Case in Organization of information security.

Organization X has some documentation and protocols on incident management. Duties and responsibilities have been distributed to employment. Project management is not formally documented, yet everything is effectively managed in practice.

3.3.1 Information security roles, responsibilities and segregation.

It is essential to clearly outline and assign all information security duties. These responsibilities can surround broad aspects, such as safeguarding information, and may also involve specific tasks, like the responsibility for granting permissions and access. Having this documented and defined is a must-have to meet the ISO27001 standard. Reviewing responsibilities after employment and regular check-ups is crucial for information security and to avoid unnecessary access. Leading into segregation of duties, to minimize the chances of unauthorized or unintentional modification or misuse of organizational assets, it is crucial to segregate conflicting duties and areas of responsibility. Maintaining a well-documented protocol on this subject facilitates a smooth ISO 27001 audit process.

3.3.2 Contact with authorities and contact with special interest groups.

In this case, nothing is mentioned about this subject, meaning the organization probably has not considered it. The organization needs to consider its business requirements and security requirements, which are bound by legislation or contractual agreements, and based on that list all needed contacts. Having a documented list of all crucial contacts in different scenarios is a good way to implement this standard requirement. Documentation should also contain the protocol about who and when to contact the authorities or special interest groups.

3.3.3 Information security in project management.

Having a practical procedure is a starting point for entering the audit. Meaning only the documentation of the procedure needs to be done. Reviewing the procedure to the standard while documenting it would be highly recommended to ensure compliance. Especially examine whether all individuals engaged in projects are assigned the responsibility to address information security throughout every phase of the project lifecycle.

3.4 Case in mobile devices and teleworking

Entering an ISO27001 audit, the only thing the organization X should look at here is that they have a clear policy on mobile devices and teleworking. Crucial for information security within the company. Without a defined and documented policy, it is impossible to pass this requirement.

3.4.1 Mobile device policy and teleworking.

It is necessary to implement a policy along with corresponding security measures to address and manage the risks associated with the use of mobile phones and other mobile devices like laptops and tablets. Consider the BYOD aspect, whilst making the policy. Education, training, and awareness regarding the use of mobile devices in public spaces are crucial factors. This includes being cautious of free Wi-Fi that may swiftly compromise information and taking measures to prevent unauthorized observers from viewing the screen during activities like public transport or cafés. These are all the things you need to consider and have documented in the mobile device policy.

A teleworking policy along with corresponding security measures should be enforced to safeguard information accessed, processed, or stored at teleworking sites. Teleworking means homeworking and other off-site activities, such as working at supplier or customer sites. It is crucial to provide teleworking staff with education, training, and awareness regarding potential risks. This needs to be documented within the policy.

3.5 Case in Human resource security.

HR security plays a crucial role in ensuring the protection of employee data and maintaining the confidentiality, integrity, and availability of HR-related information. In this case, the HR department has clear protocols that are well documented, but it is still recommended to review the documents and compare *them against the ISO27001 standard. Interviewing the head of the HR department would be highly beneficial, before conducting the full review of human resource security.*

3.5.1 Screening and Terms and conditions of employment.

Drafting and executing employment contracts should consider organizational information security. Topic-specific policies should be designed to enhance privacy protection at the departmental level. Consider having extended and defined protocols on responsibilities, NDAs, and legal obligations.

3.5.2 Management responsibilities and Disciplinary process.

Establish transparent protocols outlining managerial responsibilities, particularly in the realm of information security. In the event of an incident or legal matter, this clarity is crucial and must be explicitly defined. Disciplinary procedures should strictly adhere to these protocols, with the presence of an HR department member. Ensure that the staff comprehends the consequences of disregarding predefined rules, thereby reducing the likelihood of intentional or unintentional data leakage.

3.5.3 Information security awareness, education, and training.

The process of enlightening users on the importance of information security and inspiring them to elevate their computer security practices is vital for fostering an organizational culture of information security and ensuring comprehensive company-wide information security. This concern can be effectively tackled through proper onboarding measures. A documented and well-defined onboarding protocol, encompassing all necessary elements, contributes to successfully passing the ISO27001 audit.

3.5.4 Termination or change of employment responsibilities.

Highlights the importance for organizations to clearly outline information security duties and responsibilities that endure even when personnel change roles or move to a different department. This should be specified within a documented protocol during departmental transitions. Contract termination should adhere to non-disclosure agreements or other contractual obligations for the specified timeframe within the contract.

3.6 Case in Asset Management.

Asset inventory is maintained in a cloud log, with ownership clearly indicated when assets are distributed. However, there is a lack of a defined protocol for the return of assets, and no written policies on this matter exist. The responsibility for asset management is not explicitly outlined; currently, only the user of the asset bears responsibilities.

3.6.1 Inventory of assets, Ownership of assets, and return of assets.

The initial cloud inventory of assets with marked ownership serves as an excellent foundation for the audit; however, the remaining aspects are notably deficient and would not meet the required standards. Managing the return of assets could be incorporated into an offboarding document.

3.6.2 Acceptable use of assets.

It is imperative to formulate and implement an acceptable use of assets policy within the organization to meet ISO27001 audit requirements. Failure to do so may result in non-compliance. This policy specifically outlines the sanctioned use of organizational assets, ensuring their proper and secure utilization to protect both company resources and information. Key areas such as asset care, authorized usage, remote access, network usage, and consequences of violations are in need to be defined for clarity and adherence.

3.7 Case in Information classification.

An information classification scheme is established, playing a pivotal role throughout various aspects of the ISO27001 audit for the entire organization X. While the labeling of assets is not explicitly mentioned, certain information is subject to an active classification measure.

3.7.1 Classification of information.

Although everything seems in order, it is recommended to undertake a comprehensive review. The classification scheme needs to account for the sensitivity and importance of information, aligning with the organization's business needs and adhering to security requirements. It should consider factors such as confidentiality, integrity, and availability of information to appropriately categorize and manage data based on its criticality and impact on the organization. Also focus on the levels and authorization within the classification scheme. Ensure that the classification scheme preserves an appropriate balance between the business needs for information and the security requirements for each information category.

3.7.2 Labeling of information.

The absence of mention regarding the labeling of information is a significant issue that requires attention. Labeling information in accordance with its classification is instrumental in determining authorization levels and ensuring accurate assignment of access permissions. Proper labeling is critical for maintaining information security and streamlining workflow within the organization. It plays a pivotal role in preventing the disclosure of highly sensitive information, mitigating the potential for severe damage to the organization.

3.7.3 Handling of assets.

This matter can and should be tackled within the acceptable use of assets policy (3.6.2). In managing assets, it's important to deliberate on access restrictions corresponding to each classification level. It is imperative to keep an official record of individuals authorized to receive assets and to guarantee that IT assets are stored as per manufacturers' specifications. The proper marking of media and data for authorized parties is a crucial aspect.

3.8 Case in Media handling.

Organization X is cloud-based. There is currently no documentation or specific definition in place for media handling. Organization X has instead depended on the awareness and education of its employees to maintain this to an accepted standard.

3.8.1 Management of removable media and Disposal of media.

Clear protocols regarding removable media and the disposal of media must be established and documented. Special attention should be given to ensuring the safe disposal of classified media. While having awareness and education on the matter is beneficial, it is insufficient to meet the ISO27001 standard. Documentation is a prerequisite and a standard across all ISO 27001 categories. Without proper documentation or evidence, compliance is not achievable.

3.8.2 Physical media transfer.

Acknowledge the current or potential use of physical media transfer within the organization. If the organization categorically rejects the utilization of physical media transfers, the option to exclude this requirement is viable. However, adopting documented protocol remains a valuable option to maintain ISO27001 standards. This approach ensures that, even if physical media transfers are not in use currently, a well-established protocol exists in case the need arises in the future. This proactive measure reduces the likelihood of unintended mistakes or data leaks during such transfers.

3.9 Case in Access control.

Organization X has a team dedicated to overseeing system access and providing necessary permissions. Nevertheless, assessments and ongoing monitoring of access management are infrequent, typically only conducted during off-boarding procedures. Despite this, an up-to-date and well-maintained log is consistently kept for access control.

Critical system access points are carefully managed for network access, and the router is safeguarded with established security measures, along with ongoing monitoring.

3.9.1 Access control policy.

In the scenario provided, the absence of an access policy is a significant gap. An access controls policy is essential as it outlines the principles and components necessary for effective access management. For instance, the access policy should articulate the procedures for authorizing access and maintaining control through regular reviews and audits. This serves as crucial evidence to validate that access control is appropriately configured and upheld within the organization, ensuring information security and promoting awareness.

3.9.2 Access to networks and network services.

Based on the information presented in the case, the current setup seems to be well-organized. The implementation of restricted access and ongoing monitoring for essential access points is a commendable practice for the secure use of network devices, both on-site and off-site. Nevertheless, there is no mention of the usage or safety of public networks, raising concerns that need careful examination. It is imperative to prioritize the establishment of secure connections rather than relying on public networks, which may expose the device for invasive information collection. Additionally, the consideration and incorporation of VPN usage should be explored, particularly for off-site activities.

3.9.3 User registration and de-registration.

Implementing a formal user registration and deregistration procedure is essential, especially if not already established. An efficient user ID management system includes the capability to connect individual IDs to real individuals, as well as limit shared access IDs, with necessary approval and documentation. Integrating this process into the onboarding and offboarding procedures ensures consistent adherence to protocols. The absence of a clear protocol for deregistration can lead to potential harm if not managed appropriately. Maintaining a list of individuals with access during onboarding serves as a valuable tool for facilitating a safer and more efficient deregistration process.

3.9.4 User access provisioning and Management of privileged access rights.

The provisioning and revoking process should have the following components: securing authorization from the owner of the information system or service for its utilization, validating that the granted access corresponds to the responsibilities of the role, and preventing provisioning before the authorization process is fully completed.

3.9.5 Management of secret authentication information of users.

Tight control is essential when employing privileged access rights, given the extra capabilities usually given upon information assets and their controlling systems. This incorporates the authority to delete work or have a substantial impact on information integrity. It is crucial that such usage aligns with formal authorization processes and complies with the access control policy. The utilization of administrative users should be severely restricted, especially in daily operations. Implementing specialized monitoring procedures for administrative accounts is strongly recommended.

Having protocols set in place to confirm a user's identity before issuing new, replacement, or temporary authentication information is crucial. Any default authentication information supplied with a new system deployment should be changed promptly and follow cryptographic guidelines when implemented.

3.9.6 Review of user access rights and Removal or adjustment of access rights.

Owners of assets need to periodically assess users' access rights, both in response to individual changes, adjustments, removal, and during broader audits of systems access.

3.9.7 Use of secret authentication information.

Safeguard confidential secret authentication information. Refrain from creating accessible records for unauthorized parties. Change it promptly if there are indications of potential compromise. High-quality passwords that meet the minimum length and strength requirements outlined in the password policy or cryptographic policy.

3.10 Case in System and application access control.

To effectively review a case involving system and application access control, it's essential to consider various aspects to ensure the confidentiality, integrity, and availability of information. This is tied heavily with access control and the previous part.

3.10.1 Information access restriction.

Ensuring compliance with the access control policy is crucial when providing access to information and application system functions. Key considerations are implementing role-based access control, defining access levels, designing application menu systems, specifying read, write, delete, and execute permissions, managing the output of information, and establishing physical and/or logical access controls to safeguard sensitive applications, data, and systems. Several elements of this can be incorporated into the classification scheme and its associated protocols.

3.10.2 Secure log-on procedures and Password management system.

The structure of a secure logon must be resistant to easy bypass, with authentication information transmitted and stored in an encrypted manner to prevent interception and misuse. Enforcing a password management system is essential, guaranteeing the use of high-quality keys and passwords. It is highly advisable to articulate these requirements in the cryptography policy, ensuring that safety measures align with established guidelines and ISO27001 requirements.

3.10.3 Use of privileged utility programs.

Utility computer programs possessing the capability to override system and application controls must undergo strict control measures. This involves stringent access control, continuous monitoring, and maintaining detailed logs during usage. The extent of control measures implementation should be determined based on the risk assessment, ensuring alignment with perceived risks.

3.10.4 Access control to program source code.

Limited to individuals requiring access to the source, such as the development team or project head, stringent restrictions should be enforced to enhance source code security. This entails keeping the source code off operational systems, maintaining logs of changes to the source and instances of access, and conducting timely audits.

3.11 Case in Cryptography.

Organization X enforces cryptography controls and has an operational policy. The policy's compatibility with ISO27001 has not been assessed. Key management is currently administered solely through a key management program, with no specified protocols or documented procedures.

3.11.1 Policy on the use of cryptographic controls.

The policy needs to be reviewed to see if it is up to standard with the ISO27001 and business requirements. Use of encryption needs to be defined within the policy and serves as a valuable resource for defining business requirements regarding when encryption is necessary and the standards to be employed.

Essential to also consider legal obligations and risk assessment related to encryption.

3.11.2 Key management.

Keys should be thoroughly considered and implemented across their entire lifecycle. A crucial component is the protocol, which encompasses the oversight of cryptographic key material, including creation, distribution, alterations, backup, storage, end-of-life management, and eventual destruction. It is imperative to clearly and comprehensively document and define all phases, facilitating an easy-to-follow protocol. This not only enhances the cybersecurity culture within the organization but also safeguards a critical defense against malicious attacks.

3.12 Case in Physical and environmental security.

In this instance, well-defined protocols have been established and recorded to safeguard both employees and the business. Attention has been given to office safety, including measures such as securing doors and addressing fire safety concerns. Organization X is currently in the process of relocating its office, meaning that new measures are needed and evaluations.

3.12.1 Physical security perimeter and Physical entry controls.

Security perimeters and boundaries comprise areas containing either sensitive or critical information, along with crucial assets. These specific areas necessitate a physically secure perimeter, complete with access controls, monitoring, and comprehensive entry logs. This can be on and off premises, meaning teleworking areas need to have considerations. For example, having a clean desk policy established on and off premises.

Physical entry controls must strictly limit entry to authorized personnel only. The process of granting access must be thorough, tested regularly, and closely monitored. Documentation and logs concerning the entry and exit details of premises should be consistently monitored and logged. It is advisable to establish a system that notifies visitors when they have been on-site. This could take the form of a guest policy outlined in section 3.11.2.

3.12.2 Securing offices, rooms, and facilities.

Having addressed 3.11.1 in line with physical controls, the initial measures to secure offices have been implemented. Ensuring office security entails considerations such as noise cancellation, guest policies, and the deployment and usage of cameras and other information-gathering devices. Encouraging staff vigilance and prompt reporting of anything unusual is crucial. These measures heavily depend on location and the risk assessment conducted by the organization to determine necessary protocols. Preparedness to justify implemented or excluded measures may be required if necessary.

3.12.3 Protecting against external and environmental threats.

The premises must account for environmental or external threats, a consideration crucial to ensuring security. This necessity is contingent upon the organization's risk assessment, which, if conducted thoroughly and tailored to the premises' known risks, you should align with the ISO27001 standard. Documentation detailing these risks and the corresponding mitigation measures must be included.

3.12.4 Delivery and loading areas.

The organization does not have any delivery or loading areas, meaning in their current state they could exclude this section from the audit. A justification for the exclusion report needed to be drafted. If this were to change clear protocols and security measures need to be enforced. A recommended practice is to attempt to isolate the area from other sections and to prevent unauthorized personnel from accessing the main premises. Implementing strict controls on incoming and outgoing packages and ensuring these are governed by established protocols is essential.

3.12.5 Siting and protection of equipment.

Equipment must be positioned and protected to mitigate risks from environmental threats, hazards, and unauthorized access. The extent of protection required varies depending on the type of equipment utilized. Simple precautions, such as refraining from consuming food and beverages near ICT equipment or adjusting screen viewing angles to minimize exposure, can be effective. However, more robust security measures, including physical controls, may be necessary for certain equipment, such as server racks. Server racks should feature clear cabling to detect external devices, physical access controls to prevent tampering or theft, and temperature and humidity controls to maintain equipment integrity. Understanding your equipment and conducting a risk assessment are essential for determining appropriate positioning and protection measures. These measures should be enforced through policies such as acceptable use of assets and access control. Thorough documentation is crucial for ensuring compliance with ISO27001 standards.

3.12.6 Supporting utilities and Equipment maintenance.

Equipment must be safeguarded against power failures and other disruptions stemming from failures in supporting utilities. For instance, risks associated with failing or faulty power supplies should be evaluated and addressed. While some premises may face circumstances beyond their control, it's essential to ensure appropriate measures are in place to mitigate the impact of failures. This may include establishing protocols for contacting responsible parties in the event of a failure, restoring systems to normal operation, and implementing any necessary security measures upon resuming online activity.

Maintenance procedures for equipment vary significantly depending on the specific type of equipment being used. It is essential to have appropriate procedures in place for different types of equipment and to ensure that employees grasp the significance of equipment maintenance. This may involve tasks such as software package updates or system updates, as outdated software on critical equipment poses a security vulnerability and can lead to unintended consequences.

3.12.7 Cabling security, Security of equipment, and assets off-premises.

Power and telecommunication cables, which transmit data or support information services, must be safeguarded against interception, interference, or damage. Other cabling security measures would be cable management, to help detection of external devices near the equipment.

A frequent vulnerability arises when working outside the premises, requiring adherence to the same protocols for equipment security both on and off-site. This entails maintaining secure network connections, appropriately siting and safeguarding equipment, and adhering to clear desk/screen policies.

3.12.8 Secure disposal or reuse of equipment.

When disposing of equipment that held sensitive information, it's crucial to either physically destroy data-bearing devices and components or securely wipe them using suitable tools and technologies. This process needs to be adequately managed in the reuse of equipment as well. If a third-party company is responsible for asset disposal, ensure that all procedures are conducted to the required standards and obtain a certification of destruction upon completion.

3.12.9 Unattended user equipment, clear desk, and clear screen policy.

Unattended equipment must adhere to safety protocols. What measures are in place to secure unattended equipment, and what criteria define when equipment can be left unattended and when it must be supervised? Basic precautions such as locking laptops when left unattended are crucial. However, conducting a thorough assessment of the safety of the location is vital in this regard. If a location appears unsafe for leaving equipment unattended, it is advisable to refrain from doing so. Clearly defining employee awareness and responsibilities is essential to mitigate unnecessary risks. Mentioning unattended equipment within the acceptable use of assets policy is recommended, with the option to include the clear desk and screen policy as a subsection within this policy if desired.

3.13 Case in Operations security.

No specific case will be provided due to security reasons. Operations security is case by case specific, meaning giving an example here would not benefit the reader. Instead, we will offer best practices, ISO27001 requirements, or other recommendations to address security concerns.

3.13.1 Documented operating procedures.

Documenting operating procedures is an essential requirement that must be fulfilled. The documented procedures should be accessible to all relevant parties. This ensures that existing staff can make informed decisions when in doubt about the correct procedure and facilitates quicker and more effective onboarding for new staff. The documentation available needs to be always kept up to date to provide changing or new staff with the correct procedures to follow.

Areas of the business requiring documented procedures are those where information assets are vulnerable to risk due to incorrect operations, as should be highlighted during the risk assessment. Some of these areas are often missed when documenting operational procedures. It's important to ensure that all areas have accurate procedures in place and a clear understanding of associated risks.

3.13.2 Change management and Capacity management.

Change management procedures are one of the most crucial processes within an organization. This implies that correct protocols are followed and well documented during change management. Effective change management is crucial in most environments to guarantee that changes are suitable, efficient, appropriately authorized, and executed in a way that minimizes the potential for either intentional or unintentional compromise. Maintaining logs of change management is an essential requirement, mandated for the ISO27001 audit. These logs must include timestamps, authorization details, and comprehensive documentation of the change itself.

In change management, it's advisable not to complicate the process too much. However, it must incorporate appropriate controls and protocols to safeguard information security.

Capacity management should be approached cost-effectively and aligned with business needs, while ensuring robust security measures are prioritized. The three primary areas of concern in capacity management are communication, data storage, and power capacity. Implementing monitoring systems and alarms across all these categories helps minimize the risk of unexpected issues or service interruptions. If other categories are identified within the company implement the same measures on them as well.

3.13.3 Separation of development, testing, and operational.

Development, testing, and operational environments need to be segregated to mitigate the risks associated with unauthorized access or alterations to the operational environment. A recommended best practice is to prevent development from directly accessing the live build. Instead, when testing and development are ready for deployment to the live environment, establish a protocol and designate a responsible individual for managing the live build. This approach ensures that security measures are implemented and unintended modifications to the live service are avoided.

3.13.4 Controls against malware.

Every organization in today's world has some sort of control against malware, but the levels can vary to a high degree. The ISO27001 standard requires effective measures to defend against malware, including detection, prevention, and recovery controls, which should be deployed alongside user awareness initiatives. Identifying potential sources of malware is essential for implementing effective controls against such threats. This is typically addressed through employee awareness programs, which may include guidelines on avoiding suspicious activities such as clicking on email links or downloading unauthorized software.

3.13.5 Information backup.

From previous sections, we understand that the company operates to a significant extent in the cloud, as evidenced by their physical transfer policy case. Consequently, the development of information backup strategies becomes pivotal and should be customized to align with business needs and risk assessments related to information unavailability. It's imperative to conduct regular testing of these strategies, with evidence of such testing required during audits. Additionally, routine checks on backups are regarded as best practice.

3.13.6 Event logging.

Simply put, event logs documenting user activities, exceptions, faults, and security incidents must be generated, maintained, and routinely reviewed. Having special logs and controls on high authorization accounts is advisable, such as admin users or super users.

3.13.7 Protection of log information, and Administrator and operator logs.

Log data may contain critical and sensitive information, necessitating the implementation of appropriate security measures and access controls. This is essential to prevent tampering, which is imperative for maintaining the integrity and usability of logs as evidence.

Administrators and operators, as previously mentioned to a degree in section 3.13.6, require protection, and regular auditing, and should not be frequently utilized. Alarms on their usage and auditing are highly recommended.

3.13.8 Clock synchronization.

If the organization X operates solely within one time zone, this requirement may be excluded. However, if the organization spans multiple time zones, it becomes essential. This is due to the necessity for accurate event logging, updates, and other changes made within the organization, or the services provided.

3.13.9 Installation of software on operational systems and restrictions on software installation.

Procedures need to be established for managing the installation of software on operational systems. It's crucial to ensure that the installation of software on operational systems is formally regulated. Restrictions on software installation can be implemented to help ensure the security of operating systems. Initially, the aim is to limit the installation of non-essential software and establish a protocol for determining the necessity of any new software installations.

3.13.10 Management of technical vulnerabilities.

It is imperative to promptly identify vulnerabilities within the information systems being utilized, assess the organization's exposure to these vulnerabilities, and implement appropriate measures to mitigate the associated risks. Any vulnerability represents a security weakness that must be addressed effectively and efficiently, particularly when the risk levels are high. Poor management of technical vulnerabilities can result in considerable harm to organization X, both financially and in terms of integrity.

3.13.11 Information systems audit controls.

Audit requirements and activities for verifying operational systems should be prearranged and agreed upon to minimize disruptions to business processes. Personnel affected by the audits should be informed, and having a clear schedule for these audits promotes workflow efficiency and ensures that they are done on a regular basis.

3.14 Case in Communications security

Ensuring secure communication is integral to overall organizational security. Primary communication channels within the company include Telegram, Teams, Outlook, and company email. While organization X places significant emphasis on awareness training and onboarding, addressing aspects of communication safety, which is currently in a lack of documentation or established protocols.

3.14.1 Network controls and Security of network services.

Section 3.9.2 and the assessment based on that should cover partly this requirement. An in-depth dive is still necessary here and a review needs to be conducted. The organization should utilize appropriate methods to protect information in its systems and applications. Network controls must be carefully customized for business operations and security requirements. This may involve secure router utilization, departmental network segmentation, monitoring network access, and implementing access control measures. Effective implementation of measures is enhanced when a risk assessment of the section is conducted beforehand. Documentation and protocol need to be implemented on the measures taken to achieve the ISO27001 standard.

3.14.2 Segregation in networks.

Network segregation implies that the entire organization is not placed within the same network section. Establishing a network architecture is essential for ensuring the safety of an organization's networking. For instance, the development team can be placed in a separate network, and their test environment should be set up in a different network for enhanced security.

3.14.3 Information transfer policies and procedures.

Established transfer policies, procedures, and controls are essential to safeguard the information transfer across various communication facilities. Regardless of the communication method employed, it is crucial to recognize and address the security risks associated with the confidentiality, integrity, and availability of the information. The utilization of encryption or encrypted messaging should be clearly defined, and additional protocols should be established. Consider the classification scheme while drafting the information transfer policy to ensure correct level of encryption and to prevent the misuse of classified information.

3.14.4 Agreements on information transfer and confidentiality or nondisclosure agreements.

Earlier sections of this case review have addressed information transfer, but a reassessment is necessary to meet the ISO27001 requirement. It is essential to have protocols in place for the transfer of information, whether done digitally or physically. Moreover, agreements should address the secure transfer of business information between the organization and external parties.

Confidentiality and nondisclosure agreements have not been explicitly outlined, indicating the need for a comprehensive review. It is advisable to consult the organization's legal team to gain a clearer understanding of the business requirements regarding this matter. Requirements for confidentiality or non-disclosure agreements, aligning with the organization's information protection needs, should be identified, regularly reviewed, and documented.

3.14.5 Electronic messaging.

All information engaged in electronic messaging must be adequately safeguarded. The organization ought to establish a policy delineating the suitable forms of electronic messaging for different types of transferred information. This policy should align with access controls, secure authentication policies, log-on procedures, and information transfer policies. If desired, the organization can incorporate this as a subsection, such as within the information transfer policy.

3.15 Case in System acquisition, development, and maintenance.

The development process involved collaboration between another organization, which is a reputable software development company. The organization was selected through a process based on their experience, expertise, and proposed solutions. The system is partly controlled by the development team from another organization. Security measures are taken in-house.

During the development phase, regular progress meetings were held to ensure alignment with the project requirements and timelines. Open-source technology was utilized. Continuous testing and quality assurance measures were implemented to identify and rectify any issues promptly.

Post-implementation, regular audits were conducted to evaluate the performance, security, and compliance of the system. Maintenance and updates were carried out as needed to address any issues, incorporate new features, or comply with regulatory changes.

Based on the case there are a lot of question marks looming around the subject of security. A development policy needs to be in place for both parties to ensure correct measures are taken throughout the development and up-keep process.

3.15.1 Information security requirements analysis and specification

Security requirements and analysis should come before the implementation of development solutions to mitigate risks associated with the development process. It is essential to clearly document and establish mutual agreement on security requirements to serve as a foundational reference throughout the development phases. Incorporating these specifications and analysis into a secure development policy is a best practice, ensuring that security considerations are systematically addressed and prioritized.

3.15.2 Securing application services on public networks.

The case does not provide specific information regarding application services on public networks. However, if such services are present, it is recommended to follow the following practice.

Information transmitted via application services over public networks is required to be safeguarded against fraudulent activity, contract disputes, unauthorized disclosure, and unauthorized modification. Considerations regarding the confidentiality, integrity, and availability of data must be considered. Decisions should be based on risk assessments as well as legal, regulatory, and contractual obligations, for example GDPR legislation.

3.15.3 Protecting application services transactions.

The recommendation remains to implement security measures for all transactions to prevent incomplete transmission, misrouting, message alteration, data disclosure, and message duplication. Encryption is also necessary if transactions contain sensitive or personal data. It is advisable to include a classification scheme in transactions to guarantee the appropriate level of protection. Lastly, monitoring transactions is advised and may be necessary.

3.15.4 Secure development policy and secure system engineering principles.

A development policy needs to be drafted to ensure correct measures are taken into consideration throughout the whole development process. Secure development policy is employed to guarantee the security of development environments and to promote the adoption of secure coding and development practices during the processes of developing and implementing systems and system changes. Meanwhile, secure engineering principles focus on principles that exist at both general and specific levels, specifically development platforms and coding languages. In any development scenario, it is essential to consider, evaluate, formally document, and mandate the selection and application of these principles. It is essential to have a customized policy that incorporates both primary areas of the requirements to shape the development strategy and to aid the security culture within the organization. Additionally, the policy should clearly outline and define the use of coding tools, programming languages, testing, and environments.

3.15.5 Technical review of applications after operating platform changes.

The case referenced regular audits, and it is necessary to perform a straightforward comparison between the ISO27001 standard and the conducted reviews to determine if they fulfill the certification requirements.

The main requirement in this section is that business-related applications must undergo comprehensive review and testing to ensure they do not negatively impact organizational operations or security. This should follow the standard change management protocols defined in 3.12.2.

3.15.6 Restrictions on changes to software packages.

When utilizing open-source software, it is crucial to restrict and manage its usage to ensure that any modifications made do not compromise the internal integrity or security of the software. Establishing a culture or policy that encourages personnel to refrain from altering software or devices, and if necessary, to do so only to a limited extent. This measure has demonstrated to enhance information security, avoiding weaknesses, and bolster defense against malicious malware.

3.15.7 System change control procedures.

Modifications to systems throughout the development lifecycle must be regulated through the implementation of formal change control procedures. This should follow the standard of the formal change management process, defined in 3.12.2. Minimize the risk of unintentional mishaps or mistakes in the development process, that could potentially compromise systems once the changes are implemented to a live build.

3.15.8 Secure Development Environment and Outsourced development.

One of the critical elements here is the segregation of environments, which involves having separate environments on distinct networks for the development team. It is essential to maintain a clear separation between live and test environments. Any use of live data in the test environment needs to have the correct security measures implemented.

Access control within and outside the development team is crucial. This aspect should also be considered when outsourcing development, as is largely the case here. It is imperative to ensure that outsourced development teams adhere to the required security measures outlined in the development policy and secure system engineering principles. Supervision and monitoring of this compliance is necessary.

3.15.9 System security testing and System acceptance testing.

Security functionality testing should be conducted during the development phase. It is essential to perform specific security functionality testing for all development activities. It is a requirement to have an appropriate authority possessing security competency and responsibility to ensure security functionality.

For acceptance testing, the tests and criteria for successful testing should be determined based on business requirements before their execution. Security testing should also be integrated into acceptance testing. Documentation of this process and protocols is required. In this case it would be crucial to define which party has the responsibility to conduct the acceptance testing.

3.15.10 Protection of test data.

Test data is indispensable for the development team and security testing to ensure a realistic test version can be evaluated before deployment. Selecting test data demands careful consideration, protection, and control. Ideally, test data should be generic and unrelated to live data. However, in certain cases, the utilization of live data may be necessary, requiring appropriate security measures to be implemented. Use of encryption might be required, if the live data contains sensitive information.

3.16 Case in Supplier relationships.

Supplier relationships will always be on a case-by-case basis and ensure the organization has taken into account the key objective of safeguarding the organization's valuable assets that are either accessible to or impacted by suppliers. In this case supplier relationships have been done and agreements have been made on a case-by-case basis but following a certain information security standard with defined responsibilities and protocols.

3.16.1 Information security policy for supplier relationships.

Policy on supplier relationships is not mentioned, but a standard of information security with defined responsibilities and protocols could easily be the policy needed. Ensure the protocols are up to the ISO27001 standard and documented and written to an information security policy for supplier relationships.

3.16.2 Addressing security within supplier agreements.

Effectively addressing security within supplier agreements involves the segmentation of suppliers. For instance, implementing a standardized protocol for freelancers or external contractors is an excellent way to ensure information security and promote awareness. It ensures they adhere to the same information security standards as the organization.

However, larger service providers typically have their own security measures, and enforcing your information security protocols on them may not be feasible. It is crucial to ensure that you obtain the required level of security from such significant service providers. A notable example is AWS by Amazon, where you can personally activate and adjust security service levels based on what AWS provides. Managing this aspect is of utmost importance, and understanding your responsibilities in this regard is essential.

Another key factor to remember when dealing with suppliers is levels of access, having this defined will help immensely with security concerns. Addressing this with especially freelancers and contractors is crucial.

3.16.3 Information and communication technology supply chain.

Organization X must thoughtfully assess potential risks associated with the nature of information and communication technology services provided. For instance, if a supplier offers critical infrastructure services and has access to sensitive information such as the source code. The organization needs to implement careful protection measures. In other cases, if only exposed to public information, fewer actions are needed. A thorough assessment is crucial for provisioning the supply chain, pinpointing potential weaknesses that require attention or elevated levels of provisioning.

3.16.4 Monitoring and review of supplier services.

Reviews and monitoring should be specific to the information at risk, as a general approach is inadequate. The organization should align its review processes with the proposed segmentation of suppliers to optimize resources and ensure a focused effort on monitoring and reviewing where it can have the greatest impact. As long as there are clear intentions and evidence of this process, the organization should pass the ISO27001 standard.

3.16.5 Managing changes to supplier services.

The handling of any alterations to the service provision by suppliers, surrounding the maintenance of existing information security policies, procedures, and controls, requires careful management. This process takes into account the criticality of business information, the nature of the change, the affected suppliers and protocols, necessitating a new risk assessment. Documenting this process in the supplier policy provides an effortless means to ensure compliance with the ISO standard.

3.17 Case in information security incident management.

Effective incident management requires well-defined protocols for various incidents, with key departments such as HR, information security, and legal teams playing critical roles. Each of these departments should establish clear protocols within their respective areas of expertise. The organization has diligently documented and established protocols for all departments, enhancing the likelihood of successfully navigating this aspect of the audit. However, it is advisable to conduct a thorough review of all materials and protocols to *guarantee the accurate implementation of measures during incident management.*

3.17.1 Responsibilities and procedures.

Established roles and protocols are essential to ensure a prompt, effective, and organized response to incidents. Ensure that the incident management is according to business needs, proactively preparing for potential organizational incidents. Perform thorough risk assessments and review business requirements to verify the appropriateness of existing procedures. Clearly outline and document both responsibilities and the established procedures to follow in the event of an incident.

3.17.2 Reporting information security events and Reporting information security weaknesses.

Employees should be familiar with their responsibilities to report and understand the protocols associated with security events or vulnerabilities. Reporting a weakness and implementing the appropriate measures is crucial for information security. Incorrect actions may result in unintended damage from identified weaknesses or events. It is essential to consistently consider risk assessment when addressing security events and vulnerabilities.

3.17.3 Assessment of and decision on information security events.

Following from section 3.16.2 assessment and decision are vital steps in information security events. Assessing the scale and severity of the incident is a large part to ensure correct actions. The actions made have the goal in mind to minimize damage or compromised data or equipment, depending on the incident of course. Adherence to GDPR and other data protection laws is essential in this context. For instance, mandatory reporting to a supervisory authority is required when the severity of an incident or event has widespread implications, such as the compromise of sensitive information like social security numbers or other private data.

3.17.4 Response to information security incidents.

The objective of the response is to restore normalcy. Timely and decisive actions are crucial to minimize damage. Effective communication with all relevant parties and authorities is essential for a successful response, ensuring that both the organization and affected parties are well-informed about the situation. Protocols and documentation on this process need to be presented when entering the audit.

3.17.5 Learning from information security incidents and Collection of evidence.

Upon receiving a reported incident, initiate the evidence collection process promptly. Gather all essential information, report it, and if required, notify a supervisory authority. This procedure guarantees accurate evidence collection and reduces the risk of vital evidence going unreported.

Learning from incidents occurs through post-incident reviews, conducted after completing the incident process and collecting evidence. Adjustments can be implemented based on the review, ensuring continuous development and improvement in handling incidents.

3.18 Case in Information security aspects of business continuity.

The information security aspects of business continuity management involve safeguarding data and systems to ensure their resilience and availability in the face of disruptions or unforeseen events. Which in this case the organizations have taken clear steps to ensure that aspect, shown in prior sections 3.11 and

3.16. Certain considerations will still require attention and assessment prior to the ISO 27001 audit.

3.18.1 Planning information security continuity.

The organization must consider various events that could potentially harm the business or the information security. After contemplating the various events and scenarios, the organization can then document the plan in the level of detail necessary and the steps needed to tackle them.

3.18.2 Implementing information security continuity.

The organization is required to document, execute, and maintain procedures, and controls to guarantee the necessary level of continuity for information security in the event of a disruptive situation. After identifying the requirements, the organization must put in place policies, protocols, and other physical or technical controls that are sufficient and proportional to fulfill those requirements. Evidence of the controls needs to be provided for the audit.

3.18.3 Verify, review, and evaluate information security continuity.

Periodic reviews to assess and validate the organization must be conducted within set timelines. Documentation providing evidence of these reviews should be presented during audits or scheduled reviews, adhering to the defined process.

3.18.4 Availability of information processing facilities.

The process of information processing facilities incorporates adequate redundancy to fulfill availability requirements. Redundancy involves deploying duplicate hardware to ensure the availability of information processing systems.

The underlying principle is that in the event of a failure in one or more items, redundant counterparts will seamlessly take over. Testing of this process is crucial to ensure safety measures. Providing evidence from the testing results will serve as a sign of correct implementation, and ensure this section is covered within the ISO27001 standard.

3.19 Case in Compliance.

Compliance is a highly customized aspect for each organization, tailored to its specific business requirements and legal obligations. Having successfully addressed sections 3.1-3.17 and meeting the ISO27001 standards will greatly facilitate preparations for this section. However, certain aspects of this section may require particular focus, such as Intellectual Property Rights (IPR). We will still thoroughly examine each section.

3.19.1 Identification of applicable legislation and contractual agreements.

The organization must maintain current documentation concerning legal statutes, regulations, and contractual agreements. These documents directly relate to business objectives. It is highly recommended to consult the legal team or a lawyer in this regard to ensure compliance with legislation and agreements. There is typically a greater extent of legislation and regulation affecting the organization than initially anticipated. Therefore, seeking advice from a lawyer is usually an excellent approach to handle this section.

3.19.2 Intellectual property rights (IPR).

The organization should establish suitable procedures to ensure compliance with all its obligations, whether they pertain to legislation, regulation, or contracts, particularly concerning the utilization of software products or intellectual property rights. The organization maintains and updates records of licenses it owns for utilizing others' software and other assets. It ensures that the maximum number of users or installations specified in licenses is not surpassed and conducts periodic audits of user and installation numbers to ensure compliance. Additionally, the organization safeguards its own IPR. Providing documentation regarding the organization's IPR is recommended.

These are prerequisites for achieving ISO27001 certification. It is essential to have documented procedures addressing matters in this section, as it ensures adherence to the correct processes and facilitates the audit process.

3.19.3 Protection of records.

This section is of utmost importance for information security within the organization. Establishing defined access controls and levels of classification is essential. Records must be appropriately labeled based on their classification or encryption requirements. The method of record-keeping, whether in the cloud or physical form, also plays a significant role. It is critical to ensure that records are adequately protected against loss, destruction, falsification, unauthorized access, or public release, with security measures tailored to the specific needs of each type of record.

3.19.4 Privacy and protection of personally identifiable information.

Key aspects to grasp when approaching this section include GDPR and other data regulations relevant to your business needs. Any personally identifiable information falls under strict regulations and the organization must comply with these rules. Consequently, the company must establish clear measures and commitments to safeguard PII appropriately. Documentation outlining the actions taken to guarantee compliance is imperative and must be in place before undergoing an audit.

3.19.5 Regulation of cryptographic controls.

The utilization of cryptographic technologies is governed by legislation and regulations in numerous jurisdictions. It is crucial for an organization to comprehend the relevant laws and regulations and establish controls and awareness programs to ensure compliance with these requirements. These steps and control can be mentioned in the cryptography policy drafted in section 3.11 and ensure it contains the necessary information and steps to ensure compliance.

3.19.6 Independent review of information security.

Regularly conducting independent reviews is an excellent method to verify that systems and protocols meet the required standards. While external parties can perform these reviews, it is not mandatory. The review process should remain neutral and impartial, adopting an outsider's perspective. Documentation of these reviews is essential, particularly in cases where changes are implemented. This documentation will serve as evidence of compliance with the requirements outlined in this section.

3.19.7 Compliance with security policies and standards.

It is critical to ensure that the security policies and standards implemented align with the ISO27001 standards, as outlined in previous sections. This alignment facilitates a smoother certification process and verifies the security policies and standards. The effectiveness and maintenance of these security policies must be demonstrated in practice. Moreover, the organization must exhibit a strong security culture, which includes conducting awareness and education initiatives to underscore the seriousness of information security. Failure to do so may result in non-compliance with regulatory requirements.

3.19.8 Technical compliance review.

Frequent assessments of information systems are necessary to verify adherence to the organization's information security policies and standards. These technical reviews should encompass various methods, ranging from testing to examining the implementation of technical protocols. Referring to the testing protocol outlined in section 3.12.3 will aid in ensuring adequate compliance with testing requirements. Regularly scheduled technical reviews and evidence of these reviews should be provided to the audit.

Closing chapter

In our deep dive of the ISO27000 series, we've delved into the fundamental frameworks and guidelines designed to bolster information security management systems. At the heart of this series lies ISO27001, the internationally recognized standard, which serves as the cornerstone for organizations seeking to fortify their cyber defenses, safeguard sensitive information, and uphold data integrity.

Planning an ISO27001 audit requires meticulous preparation, strategic foresight, and a comprehensive understanding of organizational objectives. Key elements of the audit process include defining audit scope, establishing audit criteria, building a team for the audit, conducting thorough assessments, and ensuring compliance with ISO27001 requirements. By adhering to these planning elements, organizations can streamline audit procedures, identify vulnerabilities, and implement effective risk mitigation strategies.

A systematic approach with small cases into the sections of the ISO27001 standard reveals a structured framework comprising various domains, each addressing specific aspects of information security management. Extending from security policies and risk assessment to operational controls and ongoing improvement, ISO27001 incorporates a wide range of requirements to foster a culture of security, resilience, and adaptability within organizations. By adopting these foundational principles, organizations not only will achieve ISO27001 compliance but also enhance their cybersecurity resilience and improve their credibility in the realm of information security.

The primary goals of the thesis were to aid in comprehensively understanding the ISO27000 standard and its implications for entering an audit process. Mastering ISO27001 requires a holistic approach, involving thorough comprehension of the ISO27000 series, meticulous planning of audit processes, and in-depth exploration of the standard's sections. By embracing the principles, frameworks, and requirements outlined in ISO27001, organizations can fortify their information security posture, enhance resilience against cyber threats, and achieve sustained success in today's dynamic digital landscape.

References

Building an ISO 27001-Compliant Cybersecurity Program: Getting Started with Marc Menninger.

Business case for an Information Security Management System (ISMS) based on the ISO/IEC 27000 family of standards version 5 2023 by ISO27k forum.

Information Security Risk Management for ISO 27001/ISO 27002. Author: Steve G Watkins. Date of issue 2019.

Iso/Iec 27001:2022: An Introduction to Information Security and the Isms Standard. Date of issue 2022. Author: Steve G Watkins.

ISO/IEC 27001:2022 (ISMS) Awareness Training, Author: Operational Excellence Consulting. Published Jan 22, 2023.

ISO 27000 Series, The Ultimate Step-By-Step Guide by Gerardus Blokdyk. Date of issue August 19, 2021.