jamk

Information Technology Auditing Check-list for Educational Purposes

Bachelor's thesis
November 2024
Information and Communication Technology, Bachelor of Engineering

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Description

Rebiai, Alex

Information Technology Auditing Checklist for Educational Purposes

Jyväskylä: Jamk University of Applied Sciences, November 2024, 73 pages.

Degree Programme in ICT. Bachelor's thesis.

Permission for open access publication: Yes

Language of publication: English

Abstract

In response to the fast-changing digital climate and the growing need for IT auditing skills, a structured IT auditing checklist was to be constructed to serve as an educational tool. The primary objective was to develop an IT auditing checklist from an educational standpoint, focusing on guiding students toward accurate auditing practices relevant to the Auditing, Penetration Testing, and Red Teaming course, which is organized by JAMK University of Applied Sciences. The research was an assignment proposed by the Institute of Information Technology.

Some commonly used industry standards and relevant IT auditing checklists were evaluated through qualitative research methods, and then cross-referenced to create a comprehensive checklist. As a result, two IT auditing checklists were created for differing purposes. The main checklist created for the cybersecurity course was meant to address critical areas, including network security, firewall auditing, and data protection. The second checklist serves as supplementary material to the main checklist. It could possibly be used on its own in the future for various educational IT auditing exercises.

Findings suggest that the checklists could improve students' ability to understand the basics of IT auditing while complying to the specified course criteria. Furthermore, the proposed checklist was designed for potential use in practical auditing scenarios, offering opportunities for hands-on learning and engagement with real-world cybersecurity practices. Because the second checklist was concluded to work better as supportive material, it was possible for the main checklist to match the needs of the course.

Keywords/tags (subjects)

Cybersecurity, information security, IT-auditing, auditing criteria, education

Miscellaneous (Confidential information)

jamk

Kuvailulehti

Rebiai Alex

Tietotekniikan auditointitarkistuslista opetuskäyttöön

Jyväskylä: Jyväskylän ammattikorkeakoulu. Marraskuu 2024, 73 sivua

Tieto- ja viestintätekniikan tutkinto-ohjelma. Opinnäytetyö AMK.

Julkaisun kieli: englanti

Julkaisulupa avoimessa verkossa: kyllä

Tiivistelmä

Vastauksena nopeasti muuttuvaan digitaaliseen ilmapiiriin ja kasvavaan IT-auditointitaitojen tarpeeseen suunniteltiin jäsennelty IT-auditointitarkistuslista, joka on luotu opetusvälineeksi. Tavoitteena oli kehittää IT-auditointiin suunnattu tarkistuslista opetusnäkökulmasta, keskittyen ohjaamaan opiskelijoita tarkkoihin auditointikäytäntöihin Jyväskylän Ammattikorkeakoulun tarjoamalla Auditointi, Penetraatiotestaus ja Red Team -toiminta opintojaksolla. Tutkimus oli IT-instituutin esittämä toimeksianto.

Tiettyihin yleisesti käytettyihin alan standardeihin ja olemassa oleviin IT-auditointitarkistuslistoihin perehdyttiin kvalitatiivisten tutkimusmenetelmien avulla, ja ne ristiviitattiin kattavan tarkistuslistan muodostamiseksi. Tuloksena syntyi kaksi erilaiseen tarkoitukseen suunnattua IT-auditointitarkistuslistaa. Kyberturvallisuuskurssille kehitetty päälista kattaa keskeiset osa-alueet, kuten verkon turvallisuuden, palomuurien auditoinnin ja tietosuojan. Toinen tarkastuslista tarjoaa täydentävää materiaalia päälistalle ja sitä voitaisiin mahdollisesti käyttää itsenäisesti tulevaisuudessa erilaisissa opetuksellisissa IT-auditointiharjoituksissa.

Havaintojen perusteella tarkistuslistat voisivat parantaa opiskelijoiden kykyä ymmärtää IT-auditoinnin perusteita ja täyttää samalla kurssin vaatimukset. Ehdotettu tarkistuslista suunniteltiin soveltuvaksi myös käytännön auditointitilanteisiin, tarjoten opiskelijoille mahdollisuuden oppia IT-auditoinnin ja kyberturvallisuuden osa-alueita käytännönläheisesti. Koska toinen tarkistuslista todettiin paremmin päälistaa tukevaksi materiaaliksi, oli mahdollista sovittaa päälista paremmin kurssin tarpeisiin.

Avainsanat (asiasanat)

Kyberturvallisuus, tietoturva, IT-auditointi, auditointikriteerit, koulutus

Muut tiedot (salassa pidettävät liitteet)

Contents

Figures

Tables

List of Acronyms

AIDA	Artificial Intelligence and Data Analytics
AI	Artificial Intelligence
COBIT	Control Objectives for Information and Related Technology
ECTS	European Credit Transfer and Accumulation System
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technology
NIST	The National Institute of Standards and Technology
PCI DSS	Payment Card Industry Data Security Standard
PoLP	Principle of Least Privilege
SIEM	Security information and event management
SOC	Security Operations Center
SOC 2	System and Organization Controls Type 2
SSL	Secure Sockets Layer
SYN	Synchronize
TLS	Transport Layer Security
VLE	Virtual Learning Environment

1 Introduction

Vacca (2009) stated that the demand and responsibility for information security management continue to grow steadily, driven by the fact that a majority of organizations allocate larger portions of their IT budgets to risk management and intrusion prevention. This trend is further amplified by the widespread adoption of enterprise cloud computing, where many businesses are transitioning all their IT operations to internet-connected infrastructures, which is why auditing has become a vital part of a modern organization.

Due to the rise of digitalization in the modern world, the need for auditing has become increasingly apparent. Gantz (2013) addresses that auditing can potentially aid organizations in mitigating, preventing, and assessing risks involved in digitalization. Emphasizing that the dependence on information technology is evident in nearly every company regardless of its focus. To thrive in their respective markets, these organizations must effectively manage IT assets and environments, making it essential for them to adhere to established guidelines. Auditing can be practiced across all industries using different approaches, but the conjunctive element is that all audits adhere to established guidelines to meet specific levels of requirements within their respective industries.

As stated by Boritz & Timoshenko (2014, pp. 1–3) auditing checklists are globally used to help auditors and organizations comply with various requirements set forth by standard organizations or by a defined criteria. Without checklists, auditors would have a difficult time assessing an organization adequately according to requirements and fairly judge compliance to defined standards. This is why, according to them, checklists are essential for standardizing the auditing process and reducing the margin for error. They also place importance on the fact that checklists require expertise to develop, so that they are effective for standardized auditing procedures.

A good example of checklists being utilized in standardized manner can be found in elevator maintenance. According to Shaoolian (2021), elevator maintenance is often regulated by government standards to reduce safety risks and minimize repair costs. These standards typically include periodic maintenance intervals during which elevators must be inspected. Inspections can be carried out using auditing checklists to check specific elevator components such as ensuring control

panel button functionality, the cables are in good condition and doors operate without obstruction. The research suggests that the checklists are formed from regulatory standards ensuring that all elevators are inspected according to guidelines while also simplifying the inspection process.

According to Helgeson (2009) information technology auditing is the practice of accessing an environment or a product through defined criteria. These criteria can be defined through legislations provided by governmental entities. *SFS IT vuosiseminaari* (2023) state that, similarly to global standards set by international organizations, governments can establish their own standards, which are often regulatory for organizations within their region. In contrast, some international or national standards function solely as guidelines or offer tools to assist in complying with regulatory laws and legislation set by governmental institutions (*Katakri Framework*, 2020). These regulatory standards may be specific to individual countries or to once governed by a larger entity, such as the European Union, which provides directives to its member states (Calder, 2018, p. 10). Auditing standards and methods for auditing can seem difficult to understand, making it crucial to educate people about auditing and the use of auditing checklists to provide them with a fundamental understanding of the auditing process. Which is why the research aimed to identify the established criteria used in IT auditing and develop an appropriate checklist to be used for an auditing course offered at JAMK University of Applied Sciences.

1.1 Assigner

Jyväskylä University of Applied Sciences is divided into smaller schools and institutes. Institute of Information Technology also known as the IT-Institute is part of JAMK's School of Technology. *School of Technology* (n.d.) promotes that they collaborate with partners and networks to enhance learning, competence and competitiveness in multiple fields such as Engineering, ICT, and Bioeconomy. *IT-instituutti* (n.d.) explains that they offer expertise and modern knowledge in information and communication technology, electrical and automation engineering. They seek to prioritize skill development and helping students strengthen abilities and prepare for future challenges. Cybersecurity, artificial intelligence and data analytics, programming and application development as well as robotics and electrical engineering, can be studied at the Institute of Information Technology.

The thesis was an assignment from JAMK Institute of Information Technology (*IT-instituutti*, n.d.). The results from the research can be used to help develop the Auditing, Penetration Testing, and Red Teaming course taught at Jyväskylä University of Applied Sciences (*Auditing, Penetration Testing and Red Teaming*, n.d.). The final product presented to the JAMK Institute of Information Technology was an auditing checklist consisting of criteria coaligned with course requirements and various auditing standards. Main goal for the research was to find suitable auditing criteria that could be by the course's students. The checklist should guide students in auditing the environment and to develop their IT auditing skills through practical learning (*IT-instituutti*, n.d.).

1.2 Cybersecurity at JAMK

ICT Curriculum (n.d.) explains the JAMK's bachelor's degree of information and communication technology to be made up of 240 credits consisting of basic studies, professional studies, practical training, bachelor's thesis and elective studies. By completing the bachelor's, the student is able to solve problems in your study field. There are four different specialization options available for the bachelor's degree including software engineering, cybersecurity, system maintenance and AIDA, which stands for artificial intelligence and data analytics. Studies last approximately for four years depending on the student's progression speed. During the studies, students will learn ICT development in a digital and automated society as well as to plan IT solutions ethically.

JAMK Master School (n.d.) as told by the JAMK institute, master's degree at JAMK Master School is one of the most widely known master's degrees in Finland. They provide two development paths in either management and leadership excellence or higher professional expertise. By completing the master's studies students will gain the knowledge to combine theoretical information and the practical competence through working life practices while being able to study while working. The degree consists of 60 – 90 credits depending on the degree and lasting for 1 – 3 years. *YAMK - Cybersecurity* (n.d.) states that Master of Engineering in cyber security will provide students with an extended understanding in cybersecurity by educating on defending against cybersecurity attacks and planning, implementing, auditing and exercising cybersecurity.

1.3 Study course

Auditing, Penetration Testing and Red Teaming (n.d.) is a course taught at JAMK is part of the Ethical Hacking module as a part of the ICT engineering bachelor's degree. The course consists of 5 ECTS credits and requires previous knowledge of basics of Linux, cyber security, data networks which are also taught at JAMK as part of the degree. The course is divided into three sections that include auditing, penetration testing, and red teaming. The aim of the course is to teach students the most commonly used evaluation and auditing principles as well as applying security testing in practice. While also providing students the basic knowledge about security testing criteria and concepts. The information technology auditing also known as IT-auditing section of the course focuses on the basics of data security, data protection, standardization, and auditing organizations using various tools and techniques.

The course is built on a dedicated environment known as the Virtual Learning Environment that is hosted on LabraNet network. According to *LabraNet – Study Network* (n.d.), it is an study network provided by the IT-Institute. LabraNet is a dedicated network operating independently from the main network of JAMK University of Applied Sciences. Facilitating laboratory tasks and flexible learning environments. It hosts virtualized workstations with VMware ESXI servers. The Auditing, Penetration Testing and Red Teaming course is structured on around the Virtual Learning Environment also known as the VLE environment. *Virtual Learning Environment* (n.d.) is stated to be dedicated to students for education usage. VLE runs as a part of the LabraNet study network as a locally hosted cloud infrastructure. Courses run by the IT-Institute is said to have various pre-built laboratory environments for students, which can be accessed through dedicated LabraNet workstations or through a virtual private network also known as VPN.

Auditing criteria and checklist

Choosing the right criteria for this course was done by analyzing the VLE environment and reflecting on the findings. *Showcase – Virtual Learning Environment* (n.d.) shows that the environment is a virtual representation of national cybersecurity exercise networks and systems. It consists of different virtual machines which are run on JAMK's Labranet environment made to represent e-commerce organizations and security operations center also known as SOC organizations to defend

them. Students utilize the environment to attack and defend operations in a cybersecurity exercise scenario. The researched and developed auditing checklist aimed to represent the essential criteria to conduct an audit on a similar environment compared to the VLE environment used in cybersecurity exercises as seen on (Figure 1).

The auditing checklist had to be applicable to change because the course's environment would be revitalized for the next curriculum. The assigner requested the checklist to be formed in a way to be able to audit an environment similar to the cyber exercise environment (Figure 1), but with a smaller scope. The environment was said to be audited using the auditing checklist and scored based on the amount of auditing checklist questions, students would be able to answer correctly according to course requirements. The research did not include the way specific way in which the checklist was going to be utilized, but rather the checklist questionnaire was the main topic of the research.

Researching the topic began by looking at auditing as a subject and how it is utilized in organizations. There were multiple checklists and criteria behind paywalls, but also open-source material was available. The assigner ruled out using closed-source materials or sources unavailable to students, because utilizing them for the course would be complicated. The research could have been greatly enhanced if the closed-source material was taken into consideration as some of the most commonly used standards and criteria were closed-source material.

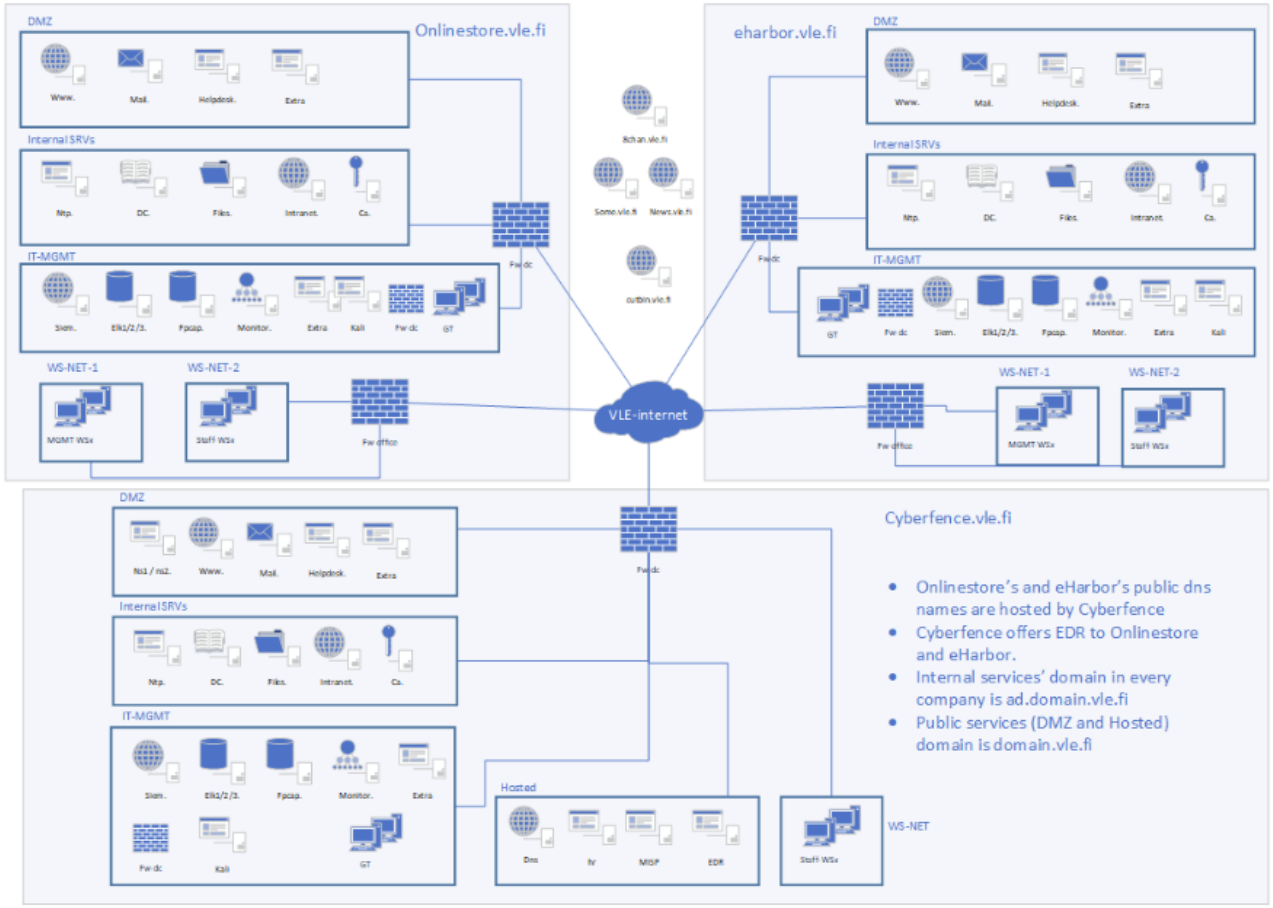

Figure 1 JAMK VLE environment (*Showcase – Virtual Learning Environment*, n.d.)

1.4 Research method

The research method chosen for this thesis was the qualitative method as it provided the most efficient techniques for researching the topic. Qualitative research is a scientific research approach focused on understanding the quality, characteristics, and meaning of the subject (*Laadullinen tutkimus*, n.d.). The method was chosen as the assigner's requirements for the topic required research into premade auditing checklists as well as the overall structure of IT auditing checklists and their requirements. As qualitative research could be described as, research that includes well-designed studies, repeated testing, and multiple perspectives can provide insights that improve understanding of both the nature of the phenomenon and its cause-effect relationships (Saaranen-Kauppinen & Puusniekka, 2006). Another reason for choosing the qualitative method was to hopefully benefit the study course in ways to improve learning and provide the assigner tools to improve the course structure.

In reference to the (Figure 2.), the assigner had identified an issue with the course structure, and in cooperation, came up with a possible solution to improve the learning experience for the students undertaking the course. Then the researcher was tasked with developing a solution in form of an IT auditing checklist for the course, with the assigner's defined requirements. The requirements were to use premade auditing checklists and criteria, then to cross-analyze the findings to find similarities within the checklists to factually identify viable questions for an IT auditing checklist. Other requirements were to use open-source material and to leave physical security related topics out of scope, as the course focus was on information security. The developed checklist results would then be presented to the assigner, and possibly used in future iterations of the course if found relevant and viable for educational purposes leaving the demonstration of the artefact and evaluation stages to the assigner (Figure 2.) and or to future research on the subject.

To summarize, the goal of the research was to develop a checklist based on the assigner's requirements, that could be possibly utilized in improving the Auditing, Penetration testing, and Red Teaming course taught at JAMK according to the course's scope. Purpose of the research was to find information on relevant auditing checklists that could be used in the development of the auditing checklist. Also, focusing on finding frequently mentioned topics between the premade auditing checklists and auditing standards. As the assigner did not place restrictions on the auditing criteria other than physical security auditing, it was left to the researcher to research commonly used auditing standards and methods of creating IT auditing checklists.

The research set out to answer the following questions on IT auditing checklists:

- What IT auditing checklists are relevant according to the assigner's requirements?
- Which subjects are frequently mentioned in the premade IT auditing checklists?

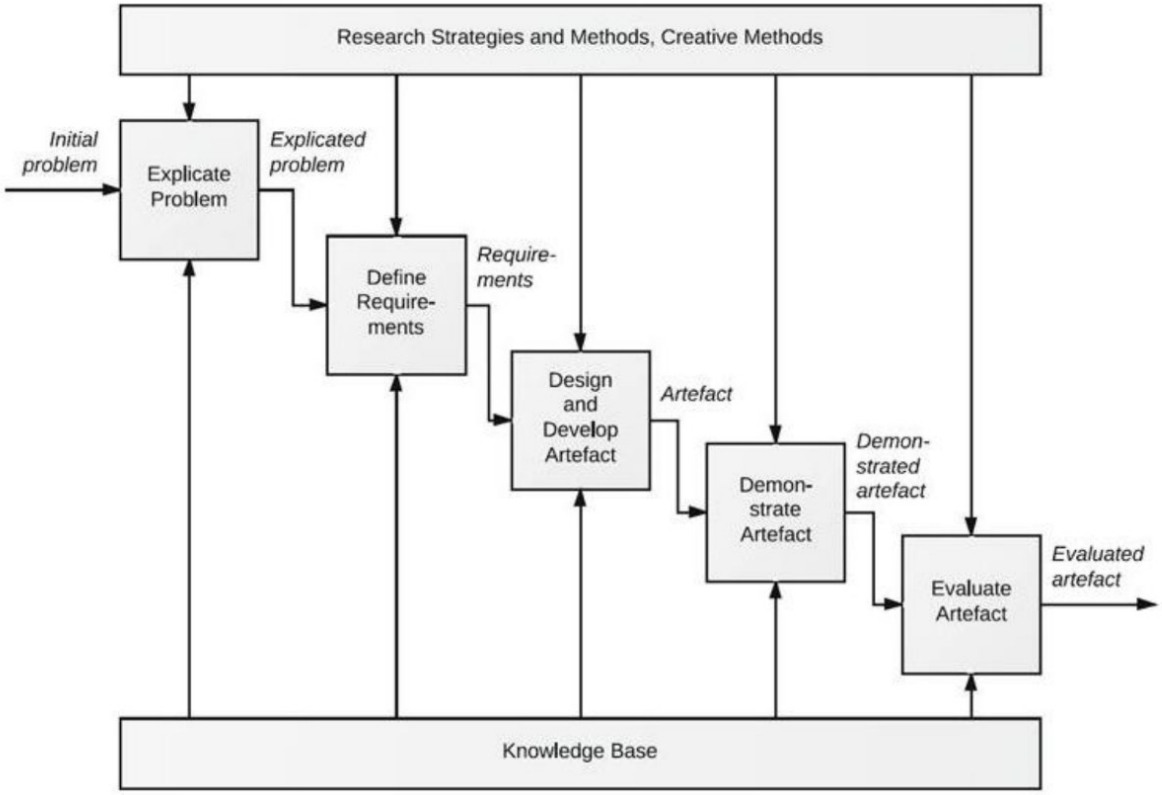

Figure 2 Method framework (Johannesson & Perjons, 2014)

2 What is auditing?

Before planning for auditing checklists, it is important to understand auditing and why it is essential for modern organizations. Gantz (2013, pp. 28 - 31) states that the definition of an audit can be described as an independent assessment, review, or inspection of a specific subject. Auditing can often be associated with the examination of an organization's financial assessment. IT auditing differentiates from regular use of the term as it focuses on auditing an organization's IT systems and procedures rather than financial status. Gantz mentions the goal of IT auditing to be providing organizations information on the status of their information security and process functionality as well as other aspects depending on auditing scopes. The purpose of audits is to assess environments to adhere to requirements and standards set by governments or industries. It is also done to ensure that controls are properly implemented to protect IT assets and information (Gantz, 2013, p. 23).

Cascarino (2012, pp. 18–19) explains that IT audit controls are often divided into subdivisions called general controls and application controls. These controls are parts of auditing scopes which help auditors in assessing organizations more efficiently. The controls should be implemented by organizations to help in maintaining organizations IT systems and processes. Providing policies and procedures on governing IT environments, systems and applications to ensure information security, integrity, availability and reliability. Cascarino states these controls to be essential for auditing organizations, and they are often good starting points when defining auditing scopes as controls like access controls and system security are a part of general controls.

Audits can be conducted internally or using external auditors to assess the organization (Kegerreis et al., 2020). Vacca (2017) explains that when conducting an internal assessment of your organization, it's important to understand that the information gathered may not be reliable. Relying on internal assessments can lead to problems due to human tendencies. He emphasizes that humans often have a hard time objectively justifying issues in their most problematic areas and environments. For this reason, it's necessary to look for independent auditors for advice and review of your organization.

Who are auditors?

Gantz (2013, p. 38) states that auditors can be described as personnel in charge of assessing various types of organizations. There are multiple types of auditors conducting audits in different fields, but IT auditors conduct assessments on IT systems. System functionality, integrity, compliance with standards are parts of auditor's job in identifying application systems (Cascarino, 2012, p. 19). Auditors can be either internal who are part of an auditing team or external to the organization depending on their role in the audit process (Kegerreis et al., 2020). Gantz (2013, pp. 38–41) explains that internal auditors are commonly people tasked with assessing and maintaining auding within the organization regularly, and external auditors are professionals expertizing in auditing different types of organizations. External auditors are qualified to assess organizations in terms of compliance with standards as well as offer certifications.

Moeller (2010, pp. 13–14) explains audit professionals to be tasked with the responsibility of reviewing and assessing management controls within enterprises. Acting as independent entities,

auditors execute tests on internal controls within enterprises and conduct a review aiming to report to management and other parties of the organizations state of security. Becoming an auditor, one must have a recognized qualification in information auditing which has been awarded by an institution that has been acknowledged by the government (Hingarh & Ahmed, 2013, pp. 4–5). Structured internal auditing performed by qualified personnel will help reduce risk to meet the customer needs and expectations if performed regularly (Coleman, 2015, pp. 3-4).

2.1 Information security

As stated in Goucher (2016, Chapter 1), computer and network technology has become widely available in the past few decades. Gone are the days of physically securing filing cabinets as the files are secured on virtually on machines and servers. Due to the fact that information is being stored virtually, organizations have started to understand the importance of information security. Goucher explains stakeholders to pressure organizations to reassure acceptable levels of security when securing information stored on virtual systems It also notes that, while the loss of sensitive data once merely caused embarrassment for a company, in modern organizations, such a loss can lead to serious repercussions and severe damage to the company's reputation and operations resulting in loss of business. As mentioned in the book, information security is a vital part of modern organizations which is why they practice information security.

What Is Information Security? (2023) state that information security also known as InfoSec, means to protect sensitive and important information to an organization from the access of unauthorized personnel. This can also include physical information security and not just digitalized information. Further explaining that the goal for information security is to provide confidentiality, integrity, and availability commonly referred to as CIA triad. These three triads represent the means to keep information secure from unauthorized users, making sure the data is not altered, and the information integrity is kept, and so that the information is kept available void of attacks like a ransomware attack which locks the data from users unless a ransom is paid (*Fortinet*, n.d.).

What Is Information Security? (2023) explain that data breaches can be extremely harmful to an organization in multiple ways. Losing customers and business is just a portion of the damage breaches can cause. In a case where sensitive data has been stolen, it will most likely become a legal matter if there’s a breach in governmental regulations for example the GDPR. For this reason,

organizations should comply with governmental regulations and guidelines to improve security. Standards provide tools and guidelines to help follow these regulations and by performing regular auditing you can prevent most common data breaches and information security risks (Merhout & Havelka, 2008, pp. 3–5).

2.2 Risk management

IIA ERM (2009) introduces risk management to be increasingly important in modern corporations. Organizations are expected to identify and explain their business risks, whether be it social, financial, operational or other potential risk factors. It is said that the use of risk management frameworks has increased as organizations realize the importance of regulated processes for management. They also explain internal auditing to serve as an insurance policy, making sure risk management is being followed accordingly by the organization. Risk management aims to enhance visibility into the overall risk posture and to highlight critical high-risk information assets and systems (Merhout & Havelka, 2008, p. 13).

Wolke (2017, pp. 1–2) states that “Risacare” meaning “to dare” is the old Italian name from which the word “risk” originates. He also explains that business literature lacks a single, cohesive definition for risk concepts, although a common definition of the term is commonly associated with possible damage or loss of net assets without any offsetting gains to balance it out. Pompon (2016) describes risk to be a way of reducing unnecessary costs and maximizing revenue. Explaining that in order to properly manage risks, it is important to understand the risks involved with the organization. While no risk analysis can be perfect even when performed by professionals, it can mitigate most common risks and reduce impact to the business.

Borek (2013, p. 18) explain that organizations must acknowledge the critical strategic significance of information risk management as an integral part of their overarching business strategies. Effectively managing information risk is crucial for organizations of all sizes and structures. Borek states it to be beneficial to create a culture where individuals within the organization actively engaged in managing associated risks, considering it an inherent part of their daily responsibilities. Failing to recognize their role in this endeavor may lead employees to either undertake actions that expose the organization to unnecessary risks or neglect activities that are essential for risk mitigation.

Audits often provide organizations with information on the risk factors and how they can properly manage risks within their organization (Gantz, 2013, p. 35). Pompon (2016) states that risk management includes numerous risk analysis and assessment methods that help reduce risk likelihood. These can be calculated by IT-professionals using different tools and tactics. They can calculate impact on the organization to develop mitigation strategies to reduce severity scale on the business. He also states that most major standards require risk analysis models to be follower using industry standards for compliance. These will be reviewed when applying for external auditing for standard certification.

3 Information security auditing standards and frameworks

Auditing should always be compared to some material that has been standardized by the industry. Meaning that auditors should use a set guideline when reviewing an organization. Helgeson (2009) states that standards are guidelines written by international, national or by the industry. These standards can be followed as guides to improve the quality of your organization. Coleman (2015) explains audits to most commonly begin by choosing specific criteria to be used in the audit. Which is done to structure the audit so that the observations are based on facts and not on personal opinion.

When choosing a criterion for your organization to follow, it's essential to establish a scope for the auditing process (Gantz, 2013, p. 152). For example, a typical medium sized organization might have separated network segments and zones under each own subnetwork implementation, with each zone containing machines and services holding important information to the organization. So, when selecting the scope for an audit process, it's necessary to assess the organizations assets, so that the correct auditing criteria can be selected for the specific audit in the planning and evidence collection stages (Gantz, 2013, p. 156). According to C. Wright et al. (2008), this process could be improved by following specific standards established by recognized auditing entities as, these standards provide reference points for the audit reporting. These standards are designed various applications, making it important to select the appropriate framework for each use case. Some of the most commonly referenced include ISO/IEC, NIST, PCI DSS, KATAKRI, COBIT, GDPR, HIPAA, SOC 2, among others, each suited for specific use cases. Research observations identified both international standards, such as ISO/IEC, and national standards, like Finland's KATAKRI framework.

The focus of this research was limited to the most commonly used auditing standards and frameworks because they provide the widest selection of specific frameworks and most information. Most often these standards are not open-source material which is why they were not included in the research, because the focus was to limit open-source standards and checklists.

3.1 ISO/IEC 27001

ISO - International Organization for Standardization (2024) ISO is an organization that provides standards for a wide range of products and services. They provide guidelines so that they can be used reliably, safely and have appropriate level of quality. The organization agrees on the best practices for different industries by gathering experts from 172 countries and has been developing standards since 1946 (*ISO - About ISO*, n.d.). IEC is another widely known standard developing and publishing organization, that focuses on all electrical, electronic and related technologies. Founded in 1906 and with 30 000 experts in 170 countries they develop standards for the electronics industry as well as many others including IT industry (*IEC*, n.d.). Together with IEC they provided a joint standard called ISO/IEC 27001 for the information security sector.

According to Vacca (2017), one of the most relevant risk management guidelines used for information security is the ISO/IEC 27001 standard. It was originally created in 2005 by two major organizations, the ISO, and the IEC. Vacca also states that the standard is updated every few years so that it stays up to date on the current requirements for organizational information security. The ISO/IEC 27000 standardization family provides organizations the guidelines to manage their asset security (*ISO/IEC 27000 Family*, 2022). Vacca (2017) details the ISO/IEC 27001 to contain a set of requirements and guidelines for managing security systems and controls. By following these rules set by the standard, your organization can receive certification after being evaluated by an approved auditor.

According to *What Is the OSI Model?* (2024), The Open Systems Interconnection also known as the OSI model is one of the accomplishments of the ISO organization. To address the importance of networking and the need for a consistent framework. In 1984, the ISO in collaboration with International Telegraph and Telephone Consultative Committee (CCITT), published the OSI model establishing a guideline for developing interoperable network solutions by introducing a layered structure that divides the network into seven distinct layers. Kegerreis et al. (2020) also describing

the model to show how data moves between systems. Explaining that it guides how to build networks to send data across platforms in physically different locations.

Due to the seemingly credible ISO standards, it was chosen for research as has been found to produce important and widely used frameworks for the IT industry. The chosen checklist provided as a Smartsheet document focuses on ISO 27001 controls. Organized into categories, this checklist template serves as an example for a comprehensive audit and also included key ISO 27001 compliance requirements which is why it was chosen for cross-analysis in the research process when complying the checklist questionnaire. Even though the ISO/IEC 27001 standard was not open source, it could be found from the JAMK library, so it was taken into consideration as it is one of the most important standards and used widely in JAMK studies.

3.2 NIST SP 800-53

As stated on the NIST website "About NIST," (2009) The National Institute of Standards and Technology was founded in 1901 to combat the challenges of other major countries in the industrial competitiveness as the U.S. lacked behind their economic rivals. NIST was later acquired by the U.S. Department of Commerce and aims to be the world's leader in critical measurement solutions and standard promotion. NIST provides frameworks and publications of topics in almost all industries and one of them is information security.

NIST framework is regarded to be one of the most prominent standards. As told on the *NIST Framework* (2014), it consists of multiple different specific frameworks and can be utilized in some way for most organizations regardless of the industry. Even though the standards in information security cannot be certified, they are still used by many organizations as they provide open-source guidance on auditing and maintaining organization's information security. Their framework documentation is being updated regularly through feedback from the industry to meet the requirements by organizations with various challenging and dynamic environments. Isaca et al. (2014) explains NIST framework to have been developed through the notion of President Barack Obama to increase security infrastructure in the most critical areas including banking systems, energy grid and secure assets. This resulted in a large framework that could be utilized in national infrastructure and by large to small businesses (*NIST Framework*, 2014). It follows principles set in ISO/IEC

27001 but has additional guidelines for different organizational sectors including management, governance, staff policies and procedures, supply chain management (Vacca, J. R, 2017).

NIST SP 800-53 provides an entire privacy and control catalogue of requirements for auditing an environment to NIST's guidelines (NIST SP 800-53, 2020). The control catalogue has extreme depth to audit even large organizations by having enough requirements to focus on all aspects of an organization's full audit. The list was selected because it offered detailed explanations on the rationale behind each specific requirement, along with sufficient topics to cross-analyze with other sources in order to form questions for the research checklist.

3.3 KATAKRI framework

Katakri is a Finnish national framework made for the assessment of an organization's ability to securely protect information. Katakri Framework (2020) describes the tool to be used by Finnish national authorities, and it can be utilized by private organizations as well. The main objective for the Katakri framework is to provide minimum requirements to organization's based on national and international information security agreements. Requirements provided in Katakri are not mandatory but consists of previous national and international information security requirements. These requirements are stated to possible be obligatory in Finland depending on the organization, but not necessarily required in other countries as they are outside of the country's area of jurisdiction.

As defined in the *Katakri Framework* (2020), it is divided into three subdivisions, security management, physical security, and information assurance. These allow for different options depending on the organization's needs. Katakri framework describes it to provide varying levels of security guidelines depending on the required security level for particular implementations. Levels are IV Restricted, III Confidential and II Secret, so that secret level is the hardest to obtain. These are solely based on Finnish national security classifications and could differ depending on the country. Katakri claims that their framework can be utilized as a tool by authorities to audit an organization's security. As the framework is nationally recognized and approved, auditors can present organizations with a Katakri certification if the obligatory requirements are met.

Katakri auditing tool provides auditors with a checklist to use when auditing environments. The checklist is divided into before mentioned subdivisions that can be used to audit specific aspects of

an organization (*Katakri Framework*, 2020). For the research subject, only division I was reviewed as it focuses on information security which was a requirement by the assigner. I division has requirements for each information security auditing topic, and they use levels of security to differentiate the requirements. As the Katakri auditing tool provides a wide range of different auditing targets and utilizes sources from other well-known standards, it was chosen to be part of the research for cross-analyzing sources for questionnaire.

3.4 PCI-DSS

PCI-SSC (n.d.) explains that the PCI Data Security Standard, commonly known as PCI-DSS, was developed by the PCI Security Standards Council, which is a global security standard development organization focusing on enhancing payment account data security. They provide payment security standards to set industry guidelines on globally securing payment data. Calder & Williams (2015) state that PCI DSS was originally founded by payment brands and implemented as an obligatory standard for all organizations who process payment transactions or hold card data directly or indirectly. While not lawfully enforced, organizations are still fined if compliance with the standard is not met. He mentions that even in cases where the business utilizes a third-party transaction service, they are obligated to verify that the third-party is following said guidelines. Compliance needs to be demonstrated by having annual security audits or submitting quarterly scans of organization's network using specific scanning tools.

PCI-SSC (n.d.) provides shortened checklists for compliance with their PCI-DSS standard on their website. These checklists most likely provide some guidance on auditing environments using PCI-DSS, but full compliance should be done by following their standard directly. The PCI-DSS requirements v 3.2.1 checklist focuses on protecting cardholder data using different techniques. Split into subcategories, an organization can focus on auditing one aspect of security at once. The checklist can be used for general IT auditing, as the principles of cardholder data security align with those of other information security audits. For example Calder & Williams (2015) state that one of the requirements is to protect cardholder data by installing and maintaining a firewall, which is a common requirement in IT security standards. Since PCI-DSS is a well-established standard, it was necessary to include it in the research for cross-analysis, serving as a primary source for the checklist questionnaire.

3.5 Zapier checklist

Abdou et al. (2021) describes Zapier as an organization providing an automation platform for applications. It is considered to be a leading business in their respective industry as it supports over two thousand widely used applications. It is marketed as a zero-coding workflow automation tool. The organization also provides featured business tips written by individuals and the Zapier IT checklist was discovered through this resource.

Zapier's IT auditing checklist was selected as a part of the research as it provided general IT auditing requirements and acknowledging general specifications needed to be considered as it provided insight into beginner friendly auditing requirements and the blog post gives guidance on the basics of auditing procedures. The checklist was not based on any specific industry recognized auditing standard which is why it was not used as main source of information, instead used to form questions for the prepared checklist or verify to claims while conducting cross-examinations.

3.6 Sprinto checklist

Sprinto as an organization provides auditing compliance automation tools for businesses with aims to achieve certification. According to Sprinto About-Us (n.d.), they launched in 2020 to help customers with complying to auditing standards using SAAS cloud dashboards for monitoring. Their tool provides metrics on compliance readiness, so that organizations can be assured that their certification is guaranteed. Sprinto also provides general checklists for specific standards and from the checklists. An ISO27001 checklist was chosen for this research as it was freely available to download and use as an auditing tool to prepare for certification process at an entry level (Anwita, 2024).

The checklist provided general information on ISO 27001 certification requirements, but did not include in-depth analysis, which is why it was used as secondary source material for checklist questions. Sprinto being an auditing compliance business, had information on IT standards, so the checklist could be considered as credible enough for cross analysis. It also provided adequate information to back up claims from the other sources in cross analysis process, hence it was chosen.

4 Conducting an audit

Audits can often require multiple stages of operations to complete fully making them time consuming and require expertise. According to Kegerreis et al. (2020, p. 45), an audit typically includes six stages, which include planning, fieldwork and documentation, issue discovery and validation, solution development, report drafting and issuance, issue tracking. Also stating the importance of proper audit planning as failure to do so will affect the outcome and reliability when performing audit reviews.

Kegerreis et al. (2020, p. 26) explain that IT auditors are people who specialize in conducting audits for organizations. They can be sourced externally through organizations providing auditing services and possible guidance for standard compliances which is why they need to understand the baseline for companies for specified baselines. They can also be internal auditors who likely spend most of their working hours focusing on components under the application layer as well as ensuring proper system security and controls for the organization.

Kegerreis et al. (2020, p. 36) state that one of the purposes of an internal auditing team is to improve internal controls within the organization. They also ensure the use of proper processes, and that systems and tools serve purposes. Internal auditors look for risks within the systems and implement controls and mitigation tactics. Internal audits follow the organization's established strategies, plans, and procedures that reflect on the organization's goals and objectives or possible audit requirements (Gantz, 2013, p.31). As Kegerreis et al. (2020, pp. 4–6) state, most often the goal for internal auditing teams is to provide assurance to the auditing committee which answers to shareholders or other relevant parties. They seek to overlook the organization and maintain required levels of internal controls withing the organization making them essential for companies.

Gantz (2013, pp. 31–32) states that external audits, on the other hand, are conducted by independent auditors who must be accredited by recognized standards organizations, as their role is to evaluate organizations against established requirements. He also highlights that external audits that focus on achieving regulatory mandates or certifications for standards, which need to be acknowledged by organizations and external auditors alike. Gantz (2013, p. 90) also describes external audits to often be performed due to regulatory demands by specific industry standards or by organizations wanting certifications by third parties. These audits have specific criteria that are

defined by organizations outside of the company and require external auditors to have full access to the organization's assets and all required material.

4.1 IT audit using checklists

Hingarh & Ahmed (2013, pp. 72–73) state that in information system auditing, it is necessary to use checklists as they provide efficient and effective outcomes on audits. They are used to perform assessments on the systems to determine the risk mitigating controls are well designed and functioning according to the risk management plans. They also explain that the use of checklists improves consistency in testing the environment for assessments performed in multiple auditing cycles. Checklist usage requires planning to decide the requirements for each auditing checklist. These criteria need to be chosen with the target environment in mind, and to allocate enough resources to audit in the planning process (Hingarh & Ahmed, 2013, p. 72). As for the researched checklist, auditing target was the focus when choosing the correct checklist questions. Also focusing on the most common auditing standard requirements, so that student can have a basic understanding of typical auditing scenarios in practice.

As told by Kegerreis et al. (2020, p. 46) while checklists can be useful for auditors and organizations planning and audit. It is important to perform a necessary risk assessment on the organization as well as alter the checklist depending on the audit scope or requirements. Organizations typically have checklists for specific systems and or environments, but they require re-evaluations before each audit. Checklists should be utilized at the start of an audit, but using methods outside of the checklists might be necessary. C. Wright et al. (2008) state that referencing established standards, checklists serve as both a guide for best practices and a way to ensure that each item aligns with specific policies and processes. This level of detail is necessary to make the checklist usable by both technical and non-technical personnel. He also explains that, developing a checklist involves understanding the organization's systems and focusing on governance and security best practices. Auditors should list references and emphasize that the checklist is based on recognized standards, improving the checklist's acceptance by the organization.

5 General IT audit checklist requirements

The requirements for the IT auditing checklist are based on the 2023 version of the ethical hacking module's Auditing, Penetration testing, and Red Teaming course. A direct one-to-one comparison to course material was not issued by the assigner, so the checklist was focused more on general IT auditing criterion made to audit a typical e-commerce company's environment, while reflecting on the (Figure 1. JAMK VLE environment). The list is a compilation of multiple auditing checklists ranging from international and national standards to documented IT coverage blog sites. Chosen topics were based on whether the specific checklist question was found in multiple sources and could be derived from cross-analyzing the material.

The checklist sources chosen for this research were from four different widely used auditing checklist tools and three different auditing standards to support some of the questions. As seen in Table 1 the tools include PCI DSS, Katakri, ISO 27001 Zapier, and Sprinto auditing checklists, while the standards comprise NIST, Katakri, and ISO 27001 IT auditing guidelines. For example, information about specific checklist requirements were researched from the internet to support checklist results. The checklist was created by cross analyzing the prebuilt checklists to identify similar questions and requirements. Items with two or more similarities were selected if they aligned with the auditing course and the assigner's requirements. This specific IT auditing checklist did not utilize any generative AI tools and was solely from direct comparisons done by the researcher. So, the checklist results reflect the finding from cross analyzing the source materials and evaluating the similarities between the requirements manually using the researcher's knowledge.

Table 1 Main checklist sources

Auditing Tools	Auditing Standards/Frameworks
ISO 27001 – (IC-ISO-27001-Controls-Checklist-10838.xlsx) https://www.smartsheet.com/content/iso-27001-checklist-templates#iso-27001-checklist	Various ISO 27001 certification guides which referred in text.
PCI DSS – (Prioritized-Approach-Tool-v3_2_1.xlsx)	NIST SP 800-53, and NIST SP 800-41 guidelines
Katakri I 2020 – (Katakri-2020-arviointityokalu.xlsx) https://um.fi/information-security-auditing-tool-for-authorities-katakri	Katakri I Framework
Zapier – IT audit checklist https://cdn.zapier.com/storage/files/ec416fa7b592dab08cb76c58758214ce.pdf	
Sprinto – ISO 27001 Audit Checklist_R2 https://sprinto.com/blog/iso-27001-audit-checklist/	

6 IT Audit Checklist

6.1 Network auditing

Question 1.1: Is the environment's network architecture secure?

Network security is arguably one of the most crucial components of IT security for any organization, as it still serves as the primary target for most threat actors (Pompon, 2016). Exploiting insecure network practices provides an easy entry point to the entire environment, underscoring the importance of strong network security measures. Sharron (2023) states that adequate network security architecture should follow industry standard guidelines and follow national mandates if required. Regularly documenting and updating the designed environment is essential, as most standards require this. Therefore, if an organization is seeking certification, maintaining proper documentation is crucial. Understanding whether a network's architecture is secure requires complete network auditing and reviewing of documentations. Also adding that, from verifying the data, an organization can deduce if their security needs to be addressed for future auditing.

Sources for the checklist question: Katakri I 401.0, ISO/IEC 27001: (13.1-13.3)

Question 1.2: Has the network been segmented and documented accordingly

A recommended practice for network environments is to segment and zone each part of the network to improve security, limit damage from cyberattacks and to protect vulnerable devices (*What Is Network Segmentation?*, n.d.). This segmentation should always be documented and regularly reviewed to ensure it aligns with the actual environment along with other inventory (*NIST Framework*, 2014). Benefits of segmenting networks are that they limit cyberattacks from extending to other zones or in the least slows down network discoverability for attackers (*Network Segmentation Using Zones*, 2024). Network segmentation can protect the most important and critical assets for an organization from malicious cyberattacks (*What Is Network Segmentation?*, n.d.).

Sources for the checklist question: Katakri I-02, Katakri-I03, Zapier "Security", ISO/IEC 27001: 13.3

Question 1.3: Does the documentation match the actual environment?

Kegerreis et al. (2020) describe documentation of the network and all its assets to be critical to an organization's security, but it is also necessary to check whether the documentation matches the actual environment. Updating the environment documentation should always be done when changes to the environment are made and during the auditing process, so there is data on previous audits. Keeping documentation updated helps discover suspicious new assets in the network because there is a record of what the environment should look like. Documentation process can be improved by using automation tools to document changes to the infrastructure as well as other changes depending on implementation (Cascarino, 2012, pp. 18). Documentation is often reviewed by external auditors in the certification compliance process, which is why documenting and updating the environment's documentation could be regarded as highly necessary (Gantz, 2013, p. 90).

Sources for the checklist question: Katakri I-03, ISO/IEC 27001: (12.1, 13.8)

Question 1.4: Is the intranet secured using segmentation (e.g., DMZs)?

According to *What Is a DMZ Network and Why Would You Use It?* (n.d.), a demilitarized zone also known as DMZ is a dedicated network section that protects the internal local-area network from

external untrusted traffic adding an additional layer of security. Secure networks should be segmented in such a way that it limits the visibility to unwanted destinations, for example configuring DMZs so that devices and services in the zone do not have direct access to other zones in the LAN. The article also explains that DMZs are built to be accessible from external sources but not the Local Area Network. This makes attacking internal services more difficult for the attackers due to the hardened DMZ and correct network segmentation. Network segmentation is a big part of network security and should be done to improve the overall security posture. Some, standards require this as a part of principle of least privilege as it serves a similar purpose.

Sources for the checklist question: PCI DSS 1.2.3, Katakri I-03, ISO/IEC 27001: 13.4-13.6

Question 1.5: Have the subnetworks been established according to the documentation?

According to Kegerreis et al. (2020), network should be segmented using practices where important traffic is sent on separate networks using tools like VLANs. This method is called sub-networking, which is a common practice for organizations. Sub-network architecture needs to be created efficiently, so that only the minimum number of IP addresses are left unused. Practically this means that when creating sub-networks, it is recommended to evaluate the required IP addresses for the specific sub-network and create the network size accordingly. In G. Wright et al. (n.d.) example, when on creating a management sub-network, it is probably best that there is not so many available IP addresses. So, if the network is 10.10.0.0, then an appropriate number of usable host IP addresses could be six if the subnet is 10.10.0.0/29 depending on the size of the organizations management network. This is done so that attackers cannot easily obtain ip addresses within the sub-networks if they have gotten access to the network. When attackers are able to change their IP address to the same sub-network as the vulnerable organization, they can impersonate users and avoid firewall detection due to the IP address being whitelisted. Proper documentation and efficient usage of sub-networks is often required by auditing standards when applying for certification.

Sources for the checklist question: Katakri I-03, ISO/IEC 27001: (13.2, 13.8)

Question 1.6: Does the data traffic flow correctly between subnetworks?

According to Kegerreis et al. (2020), to accommodate an implicated security level, corresponding network traffic filtering and monitoring needs to be applied to the organization. Meaning that filtering unwanted traffic as well as traffic towards external destinations needs to be limited. C. Wright et al. (2008) state that managing the flow of traffic should be done using firewall policies and filters which need to be verified for correctly filtering traffic to meet the environments requirements. This could include filtering traffic from internal sources to go through dedicated proxy servers to internet destinations. Chiradeep (2022) explains that DMZ would ideally be placed between two firewall and even by different vendors optimal security. DMZ enable the network to expose only a single device to the internet reducing the threat surface. For instance, users would still have access to internal services, but they would be controlled and monitored through the DMZ, limiting unauthorized access.

Sources for the checklist question: PCI DSS 1.3.4, Katakri I-02, ISO/IEC 27001: 13.4-13.6

Question 1.7: Has the management network been configured using Principle of Least Privileges?

According to NIST SP 800-53 (2020, pp. 36–38) framework publication, principle of least privileges should be used when defining the management network to minimize the attack surface for attackers. Also, this helps keeping track of the inventory in an environment so that monitoring and future IT auditing can be done more efficiently and won't be as resource heavy on the organization. According to *What Is the Principle of Least Privilege?* (n.d.), Principle of Least Privilege also known as PoLP is an information security concept stating that users should be granted access only to specific data, resources, and applications necessary to complete required tasks. Often seen as best practice for organizations, this approach reduces risk by limiting access for unauthorized personnel and preventing potential misuse that could disrupt operations. Adhering to the use of PoLP can be regulatory for most standard certifications for example PCI DSS. Implementing PoLP will most likely require extensive planning to cover all systems and services, but some changes could be relatively straightforward depending on design and solutions. For example, limiting user access to device configurations or other administrative tasks can be done by adding user roles to environments or active directory organizational units etc (Chai & S. Gillis, n.d.).

Sources for the checklist question: PCI DSS 7.1, Katakri I-02, ISO/IEC 27001: (12.4, 12.14), NIST SP 53-800

Question 1.8: Does the environment use https, TLS algorithm and other industry standards for encryption?

Verifying the integrity of the environments protocols is a critical part of auditing IT environments. The use of encrypted transfer protocols over the internet is essential and even mandatory in some scenarios. According to Lake (2019), auditing this should be done by checking the websites used by the organization and possibly limiting the use of http websites and other websites with limited encryption protocols. Explaining that Secure Sockets Layer/ Transport Layer Security (SSL/TLS) should also be enabled on email servers so that email traffic cannot be captured using man-in-the-middle attacks or other similar attack tactics. Encryption information can be verified from most email providers settings or using tools for checking SSL/TLS protocols. SSL is the precursor to TLS and the term "SSL" is still commonly used interchangeably with TLS or collectively as "SSL/TLS", even though SSL has not been updated since 1996 and is considered obsolete (*What Is SSL (Secure Sockets Layer)?*, n.d.).

Sources for the checklist question: Katakri I-04, Sprinto #4, ISO/IEC 27001: 10.1-10.2

Question 1.9: Are there measures put in place to defend against common network attacks (DoS, DdoS, etc.)

According to *What Is a Denial of Service (DoS) Attack?* (n.d.), denial-of-service also known as DoS attacks is a malicious effort aimed at disrupting or to shut down regular operations on a specific server or network. This can be achieved through sending a massive volume of requests from a single source to the target causing it to crash, resulting in system unresponsiveness and unavailability for legitimate users. These attacks are said to come in different forms each targeted towards specific use cases and understanding DoS attacks is essential for an organization's cybersecurity strategy. They explain that preventing and mitigating against DoS attacks can be done by layering defenses and using combinations intrusion detection and intrusion prevention systems to detect and

prevent the attacks. There are multiple solutions to mitigating DoS attacks according to them and having incident response and recovery plans are important.

Whereas DoS attacks are from a single source or service, distributed-denial-of-service attacks also known as DdoS attacks involve multiple compromised systems targeting an singular network or service making them harder to prevent (*What Is a Denial of Service (DoS) Attack?*, n.d.). Goldman (2023) explains that DdoS attacks should be mitigated using layered defenses by utilizing several protection methods at various points in a network as each layer can compensate for another layer's weaknesses. He states that businesses should turn to their cloud service providers for DdoS protection, but they often cannot protect application layer attacks. Goldman describes load balancers to be an effective way to mitigate DdoS attacks which may not be detected by service provider's network or Ddos protection. Load balancers serve the role of absorbing some of the impact and balancing the traffic across the network. Best practice for mitigating DoS and Ddos attacks was found to be having layered defenses and strong incident response processes.

Sources for the checklist question: Katakri I-02, ISO/IEC 27001: 12.5-12.6

6.2 Firewall auditing

Question 2.1: Does the network have firewalls and are they enabled?

What Is a Host-Based Firewall? (n.d.) describe network-based firewalls to be established in front of the environment so that traffic from the internet is monitored and filtered for malicious or other untrusted traffic. To have at least some environment security, it is recommendable to have either a network or host-based firewall configured to the environment. Host-based firewalls are more beginner friendly compared to network firewalls, but network firewall should serve as the first line of defense against threat actors or other malicious traffic. Most major standards like PCI-DSS or ISO 27001 require network firewalls to be established and enabled for certification application.

Sources for the checklist question: PCI DSS 1.2.3, Katakri I-03, ISO/IEC 27001: 12.5

Question 2.2: Are environment's firewalls up to date?

Key Firewall Best Practices (n.d.) state that keeping network firewalls up to date is one of the basic steps for security management. This includes keeping the software updated as well as the configurations, policies, protocols, and filters associated to the firewall. One of the most important aspects of security is reacting swiftly to critical vulnerabilities when they have been found. Regularly updating firewall configurations can help mitigate some security issues and ensures compliance with current regulations and standards. Also mentioning that, firewalls should be updated as the organization's assets expand to maintain standard levels of security. According to *Key Firewall Best Practices* (n.d.), organization's firewall administrators should also actively participate in conversations with the cybersecurity community and directly with vendors. Staying informed on the latest security threats can help mitigate issues. For some organizations without a dedicated SOC, it could be beneficial to have automatic updates enabled for firewalls if possible, so the risk for forgetting to update firmware and software can be mitigated.

Sources for the checklist question: Katakri I-03, ISO/IEC 27001: 14.1, Zapier "Network firewall"

Question 2.3: Does the firewall/s restrict unnecessary traffic and permit only authorized traffic?

Well thought out firewall rules and policies need to be established for the firewalls to achieve recommended security levels (*Key Firewall Best Practices*, n.d.). According to Godluck (2023) best practice for setting up firewalls is that you start with deny all by default. Then you enable only the required policies and whitelist environments connections. This prevents most common vulnerabilities as well as limits ground for malicious actors. Although this method is very effective at blocking traffic, it might cause some difficulties in the long run when trying to expand the environment. So, tinkering with the rules and policies might become a routine task. He explains that organizations should decide whether to have a default deny or default allow approach in terms of the firewall. Default allow model enables more flexibility and ease of use, but also carries security risks in terms of adding more attack surface and failure to meet compliance for most auditing certifications.

Sources for the checklist question: PCI DSS 1.3.4, Katakri I-03, ISO/IEC 27001: 13.2-13.4

Question 2.4: Has the firewall security including rules, policies, protocols and filters been tested?

Kegerreis et al. (2020) explain firewalls to be one of the most beneficiary tools in modern environments and testing their security is important. Firewalls should be routinely tested, checked, and audited to ensure that security is up to the organization's requirements. Checking this can be an extensive process so dedicating time and enough resources to it is highly recommended. According to them, testing firewalls can be done using penetration testing techniques like port scanning and packet analysis as well as manually checking the firewall and comparing it to documentations already set in place. Also adding that using auditing tools and premade checklists could potentially help in the testing. Using automated tools and Nmap scripts can reduce the auditing time and improve overall efficiency (Garn, 2024).

Sources for the checklist question: Katakri I-03, NIST SP 800-41

Question 2.5: Has the firewall rule "deny-by-default" been enabled?

According to Kegerreis et al. (2020), deny-by-default or default-deny should be enabled, if the security is the most important aspects of the environment. Although not always possible or recommended, it provides best possible security when hardening environments and should be used by all organizations. Almost all industry standard certifications require organizations to use deny-by-default rules. Deny-by-default rule blocks all incoming and outgoing traffic by default that has not been permitted, and it is the user's job to whitelist the required addresses, so every connection should be documented to make whitelisting easier (Scarfone & Hoffman, 2009). When enabling default-deny rules to all the different settings, policies and filters, it's good to keep in mind that you do not want to accidentally block your own connection to the firewall which would cause problems (Kegerreis et al., 2020).

Sources for the checklist question: PCI DSS 1.2.3, Sprinto #3, Katakri I-02, NIST SP 800-41

Question 2.6: Have the appropriate filtering policies been configured in the firewalls?

According to *What Is Firewall Configuration and Why Is It Important?* (n.d.), firewall policies need to be configured so that it limits probability of unwanted traffic causing issues for the organization

as attackers are constantly looking for outdated network configurations and open ports on servers. Scarfone & Hoffman (2009, p. 41) explain that deciding on firewall rules should be well thought out and fully documented so that there are backups of the rules, policies, protocols and other possible firewall configurations. This can also be done by reviewing firewall rules, conducting penetration testing and monitoring logs to verify the compliance with industry standards. Whether a rule is appropriate for an environment is up to the organization to decide, but approaching the task with Principle of Least Privilege in mind can ease the process. They also state that organizations should perform a risk assessment to identify the types of traffic essential for their operations and determine the security measures required for each. This includes specifying which types of traffic are permitted to pass through the firewall under what conditions.

Sources for the checklist question: Katakri I-03, Zapier "Network firewall", ISO/IEC 27001: 13.1-13.3

Question 2.7: Are there unnecessary firewall rules, policies, filters enabled?

According to Kegerreis et al. (2020), unnecessary firewall rules can cause issues for organizations because they can open ways for attackers to approach the environment as well as add complexity to the firewalls. Also adding that large quantities of firewall rules can make it hard to remove rules as it might break previously set up software and devices. For example, *IBM Security Randori* (2024) explain that having incoming traffic from high-risk ports can give ground for attackers to abuse. So, disabling ports that aren't required for the environment to work is really important. Also having monitoring on ports that are not used often is also important so suspicious traffic can be tracked and handled accordingly. According to the Scarfone & Hoffman (2009, p. 28) using deny-by-default method can automatically block some of these issues to improve security. Deny-by-default hardening technique is often required or highly recommended by industry standard organizations as it provides best practice security.

Sources for the checklist question: Katakri I-03, ISO/IEC 27001: 13.1-13.3

Question 2.8: Has the anti-virus software been deployed and updated to the latest stable version on all systems (workstations, servers etc.)?

NIST SP 800-53 (2020, pp. 334–335) describes anti-virus software to be an important part of an environment's security. Even though most larger organizations have network firewalls and host-based firewalls, it is still important to have another layer of defense in place. Even adding that it might be beneficiary to use protection tools from different vendors as they tend to update software at different times. So having a regularly maintained anti-virus software on all workstations, can mitigate most common malicious software. Daily scans of the discs and memory should be enabled and quarantining suspicious applications is a necessity (*Understanding Anti-Virus Software | CISA*, 2009). While typical anti-virus software can be a viable option for most small to medium sized organizations, it should be noted that larger organizations might prefer to use other intrusion detection and -prevention tools instead or as an addition, as they could provide better management options (*IPS. vs. IDS vs. Firewall*, n.d.).

Sources for the checklist question: PCI DSS 5.1, Katakri I-03, Zapier "Anti-virus software", ISO/IEC 27001: 12.5

6.3 Policies and systems auditing

Question 3.1: Are the assets and functionalities of the systems aligned with their intended purposes?

Stone et al. (2018) stated in NIST documentation that the more functionalities a system has, the more ground it inventible creates for attackers to possibly use. All of these assets and functionalities should be mapped and documented well so that they can be verified and compared when doing auditing. They identified a viable solution to address the issue of unregulated or unmonitored assets by controlling application usage and allowing users to request access to specific assets, while incorporating these assets into existing documentation. Speed (2012, pp. 86–88) explains that protecting assets can be equally as important, so identifying all assets and adding value should be done to understand the importance of each asset for the organization. In cases of data loss organizations need to be prepared to find the lost data, in which proper asset management can be crucial.

Sources for the checklist question: Katakri I-03, ISO/IEC 27001: 12.12

Question 3.2: Does the environments existing documentation include policies and procedures for governing risk management?

A well-documented environment can help keep track of all the risks associated with IT infrastructure (Speed, 2012, p. 163). Risk management should have documented records of all the policies and procedures related to the environment (C. Wright et al., 2008). This document could include records of risk matrixes and other risk assessments as well as the processes for mitigating risks and incidents, for example as seen in Appendix 1. Organizations should establish processes and policies for employees to follow, so reacting to incidents or other issues can be regulated, to improve business continuity (Cascarino, 2012, pp. 313–314). Most IT standard certifications require organizations to follow strict guidelines on governing risk management and how it should be documented, or in the least require an acceptable level of risk that has been documented (*Katakri*, n.d.).

Sources for the checklist question: Sprinto #1, ISO/IEC 27001: (5.1, 12.1)

Question 3.3: Has a risk matrix been developed for each identified risk factor? Have these risks been evaluated, and are there mitigation plans in place?

The risk assessment matrix helps in identifying and quantifying the risk, likelihood and impact risk of potential risks affecting the business (Vicente, 2024). Although a risk assessment matrix is not required to complete by organizations, auditors might use matrices as a part of the organization's risk assessment stage in an audit (Cascarino, 2012, p. 37). According to Vicente (2024), the risk assessment matrix is a tool for tracking security and business continuity risks by assessing the likelihood and potential impact. This matrix visualizes probability versus severity, helping calculate risk scores for each asset. Appendix 1 includes an example, listing systems and services with their highest potential risks. Compiling a risk matrix requires an organization to gather information on assets and perform testing to find out potential risk factors. This can be done using various auditing and penetration testing tools and techniques (Vicente, 2024).

Sources for the checklist question: Katakri I-03, ISO/IEC 27001: 16.1, Sprinto #2

Question 3.4: Have the devices and systems been scanned for vulnerabilities, and are regular environmental scans in place (e.g., using Greenbone, Nessus, Lynis)?

Most organizations should have a scan process where the environment is scanned periodically in addition to intrusion detection software or other continuous monitoring tools, even though can most likely detect vulnerabilities as well (Speed, 2012, p. 120). According to Kosinski & Forrest (2023), scans can be automated using some modern vulnerability scanner tools, so that it doesn't have to be done manually. Results of the scans should also be saved for further inspection and adding a reference point for future audits on the same subject. MBA (2024) state that most standards require periodical internal and external scanning at least quarterly for certification. This is often the most important aspect of auditing an organization, because it helps on finding the most prevalent issues regarding the network and systems.

Sources for the checklist question: Zapier ("testing", "IT logs"), NIST 800-53, Katakri I-03, ISO/IEC 27001: 12.15

6.4 Security/Firewall auditing

Question 4.1: Do the systems/machines lock after a specified number of invalid login attempts?

Esheridan (n.d.) claims that systems and machines should have a protection lock against too many failed login attempts in some for to protect against brute-force attacks. This can be done using various techniques for example locking a user out of the account for a specified time or using CAPTCHAs, stating that some methods are not suitable for each use case. Explaining that login protection can help in mitigation against brute force attacks, as it would require more advanced tools and greater amount of time. Some services and machines might these kinds of functions enabled by default, but checking each individually is important when auditing an organization. Also implementing false login attempt detection on services is important for monitoring as it can help in identifying threat actors or other malicious activity (*Katakri*, n.d.).

Sources for the checklist question: Zapier "Passwords", Katakri I-07, ISO/IEC 27001: 9.8 - 9.10

Question 4.2: Do password policies mandate the inclusion of alphabetic, numeric, and symbolic characters?

Require Strong Passwords | CISA (n.d.) states that small to medium sized businesses should have a minimum password strength of 16 characters for optimal security. Passwords should have upper-case, lowercase, numbers, and special characters. Additionally, the use of common passwords that are susceptible to dictionary attacks and other brute force attacks should be prohibited by the users and to require unique passwords. Almost all industry recognized standards require the use of complex passwords and changing the passwords within appropriate intervals (*Katakri*, n.d.). The use of multifactor authentication is also recommended as it provides better security (Grassi et al., 2017). Password policies often change when new regulations are put in place for example the new NIS2 establishes new regulations on password security (White, 2024).

Sources for the checklist question: Zapier "Passwords", Katakri I-07, ISO/IEC 27001: 9.9 – 9.10

Question 4.3: Do the devices satisfy the hardware requirements necessary for the programs in use?

End-of-Life Software (2016) explains the topic as often disregarded is the fact that old devices will start to develop vulnerabilities due to them having outdated specs and manufacturers having short end of live cycles. Devices that do not meet the requirements could cause issues in normal production use cases as well as, they might have hardware level exploits. Using legacy hardware could lead to the organization being susceptible to various attacks and to data loss incidents in case of hardware failure. Which is why regularly updating software as well as hardware is essential for keeping security of the environment in check. This has become even more prevalent as hybrid and remote work has become a staple in the working industry as organizations need to educate employees on correct hardware and software security management (*Ohje erillistyöasemien tietoturvallisuuden varmistamisesta*, 2023).

Sources for the checklist question: Zapier "Hardware/Virtual hardware", Katakri I-19, ISO/IEC 27001: 13.8

Question 4.4: Has IP address spoofing (replication/faking) been addressed?

According to *IP Spoofing & Spoof Attacks* (2018), IP address spoofing is one of the many types of spoofing attacks used by threat actors. Man-in-the-middle, Ddos and masking botnet devices attacks are one of the more widely known forms of IP address spoofing. These attack techniques require the attacker to modify source packet headers, so that the receiving machine reads the packets as legitimate, even though they are from the attacker. Mitigating IP address spoofing can be done by using packet filtering on network monitoring tools. Ingress and egress filtering is a reliable way to limit IP spoofing, which can be enabled in most firewall filters. So, organizations should check to see that mitigation plans are in place for spoofing attacks.

Sources for the checklist question: PCI DSS (1.2.3, 1.2.4), Katakri I-02, ISO/IEC 27001: (12.5, 12.13)

Question 4.5: Have the configurations and other critical assets been properly backed up and secured?

Modern organizations should be prioritizing proper data management, which involves utilizing backups and secure data storage methods as a part of their business continuity plan (Speed, 2012, pp. 179–180). According to *Katakri Framework* (2020, p. 104) this process includes reviewing documentations on important assets and creating backup solutions for these assets. Classified data should be backed up and protected for the entire lifecycle. Katakri requires the correct handling of backups for compliance with the guidelines. Exposure to unnecessary loss of data can possibly be mitigated by backing up organization’s critical assets and managing it accordingly.

Sources for the checklist question: PCI DSS 1.2.2, Katakri I-03, Zapier "Backups", ISO/IEC 27001: 12.6 – 12.10

Question 4.6: Are monitoring programs enabled and configured to generate alerts and warnings from suspicious activity?

According to *What Is an Intrusion Detection System (IDS)?* (2023), monitoring can be performed by using tools like intrusion detection systems which are tools that automatically alert security administrators of potential threats or by sending alerts to centralized tools. In addition, tools like intrusion prevention systems are made to block threats automatically. These tools combined can help in stopping or detecting directed attacks from suspicious actors. Most monitoring tools can be configured to have multiple points of monitoring across the network. Configuring these can be time consuming but the results greatly improve monitoring capabilities. *ISO 27001:2022 Annex A Control 8.30* (n.d.) explains that other viable solutions are outsourcing cybersecurity services which likely include active monitoring capabilities, so investing in internal cybersecurity teams is not always necessary. While outsourcing cybersecurity services can be a viable solution, it must not compromise security because standard certifications still require an elevated level of security. For example, intrusion detection system implementation is required by PCI-DSS standard for certification compliance (*What Is an Intrusion Detection System (IDS)?*, 2023).

Sources for the checklist question: Katakri I-11, Zapier "Alerts", ISO/IEC 27001: 16.1

Question 4.7: Is end-to-end encryption in place to protect against intrusions?

According to Sheldon (2024), end-to-end encryption is an effective method for guarding against man-in-the-middle attacks, tampering, and other similar threats. With a wide range of encryption methods available, it’s crucial to carefully select the appropriate encryption for each specific use case. He also explains that while encryption is essential, it's important to recognize that not all data can or should be encrypted, as doing so might create complications or add unnecessary steps to the data flow. Depending on the secrecy of the data being sent, using adequate levels of encryption is required by most standards certifications. Standards like ISO27001 require the proper use of cryptographic encryption, so compliance with adequate information security management is required for most certificates although not mandatory with GDPR (*ISO 27001:2013 – Annex A.10: Cryptography*, n.d.).

Sources for the checklist question: Katakri I-04, Sprinto #5, Sprinto #8, ISO/IEC 27001: (10.1, 13.2)

Question 4.8: Does the environment utilize continuous monitoring programs for example SIEM tools.

Continuous monitoring is often seen in larger organizations, which have their own security operations centers or buy cybersecurity services from 3rd parties. *What Is Continuous Monitoring?* (n.d.) article explains that automation tools enable these monitoring capabilities which still need to be observed by individuals. Continuous monitoring enhances an organization's security significantly and can be applied to monitor application, network, and infrastructure data. *What Is SIEM?* (n.d.-a) states that security information and event management also known as SIEM tools utilize continuous monitoring through monitoring points across the network and systems, consolidating the gathered information into SIEM dashboards for centralized viewing. Also adding that, continuous monitoring ease tracking and reporting of compliance with standards and regulations.

Sources for the checklist question: ISO/IEC 27001: 16.1, Sprinto #7, Sprinto #9, Zapier "Alerts"

Question 4.9: Have the appropriate admin privileges been provided to users using PoLP?

What Is Principle of Least Privilege (POLP)? (n.d.) guide describes the principle of least privilege also known as PoLP to often be regarded as one of the most powerful methods for enhancing an organization's cybersecurity defenses. PoLP should be adhered to when assigning user rights. Users should be divided into at least three categories which are superusers, least-privileged user accounts and guest accounts. Superusers could be the administrative accounts that are used for management and other administrative tasks and least-privileged user accounts should be administered to all other employees of the organization. Guest accounts should be reserved for temporary external use only. Most users do not require access to all tools and services.

Permissions should be granted based on necessity and revoked when no longer actively used (*What Is the Principle of Least Privilege?*, n.d.). For example, a system could possibly be established for users to request specific rights to individual services, with administrators having the authority to approve or deny these requests. *What Is Principle of Least Privilege (POLP)?* (n.d.) states

that once the administrative status of all user accounts has been verified, the data should be documented and regularly updated. This ensures that records of all accounts and their permissions are maintained, providing necessary documentation in the event of security breaches.

Sources for the checklist question: PCI DSS 7.1, Katakri I-02, ISO/IEC 27001: 9.3, Zapier "Accounts"

Question 4.2.1: Are the logs are securely stored in ways that prevent tampering?

An essential aspect of information security is the storage of sensitive and critical information. In the explanation from *Ohje erillistyöasemien tietoturvallisuuden varmistamisesta* (2023), logging material can be considered as sensitive information as it might leak critical information about the organization or customer data. This data should also be handled according to regulations for example the European Union General Data Protection Regulation if the organization is residing in European Union. Heiligenstein (2024) emphasizes that securely managing logging information is crucial, as attackers may target this data to gain insights into assets and conceal their activities through log masking, obfuscation, and tampering. Preventing attackers can be achieved by securely storing logging data on secure servers and employing robust encryption methods to prevent possible reverse engineering of the data and protecting folders with higher privileges. Often standard certifications require securely storing logs as a part of information security.

Sources for the checklist question: Katakri I-10, ISO/IEC 27001: 12.9

Question 4.2.2: Are system logs and other critical logs regularly reviewed for abnormal behavior?

C. Wright et al. (2008) explains that log reviewing can be made more efficient using centralized systems for log monitoring. These tools help to understand difficult logging especially on Windows based machines as they are notoriously hard to understand. Also, having individuals who can understand the logs of each service should be a necessity. According to *Security Log Management and Logging Best Practices* (n.d.), standard certifications often require regular reviews of logging data as standard practice for compliance. If potential security information and event management tools are established properly, reviewing logs can be done using those tools. It is important to fo-

cus on details containing signs of tampering or other obfuscation attempts. In the article, some examples of evets that should be logged were for example, authentications, access control, session activity, changes in user privileges as well as other important event that should be considered for logging.

Sources for the checklist question: ISO/IEC 27001: 12.8, Zapier "Alerts", Zapier "IT logs"

Question 4.2.3: Are critical logs being monitored using program agents or similar tools?

According to “What Is Agent Based Monitoring?" (n.d.), agent-based monitoring consists of multiple lightweight software agents that are set up across the network to continuously collect data and send them to centralized monitoring tools. There are numerous monitoring tools that can be enabled to monitor logs using agents. While agents not the only adequate solution to continuous log monitoring, centralizing logging to a single platform simplifies the reviewing process and automates tedious tasks like manually looking at individual events (C. Wright et al., 2008). *Security Log Management and Logging Best Practices | TechTarget* (n.d.) advises to collect data on critical assets and events, such as user activities and application logs, which can trigger alerts if suspicious behavior is detected. Additionally, monitoring fault detection and error logging is important if the security information and event management tool supports these functions, as system errors and other data can provide valuable insights into the overall state of the systems.

Sources for the checklist question: Katakri I-04, ISO/IEC 27001: 12.8 – 12.10, Zapier "Alerts",

Question 4.2.4: Is change detection active and functioning correctly, including file integrity monitoring and alerting users of unauthorized file modifications?

Obfuscation is the act of hiding tracks to make detection more difficult by using various methods, for example steganography or impersonating legitimate protocols (*Data Obfuscation, Technique T1001 - Enterprise | MITRE ATT&CK®*, n.d.). Therefore, enabling change detection mechanisms is crucial for effectively monitoring environments so that log data cannot be manipulated without generating alerts to monitoring systems (Vacca, 2017, p. 17). Known by various names, detection monitoring needs to be configured using different tools and or rules preventing or monitoring the

use of specific actions most commonly related to hiding tracks (*About Detection Rules | Elastic*, n.d.). These obfuscation techniques could be caught by for example monitoring the changing of certain file names, detecting PowerShell commands and signs of lateral movement (*PowerShell Detections*, 2021). Proper configuration should be done by following guides from industry recognized standards and service provides as they might provide checklist guidance on configuring the correct rules.

Sources for the checklist question: PCI DSS 11.5, Katakri I-04, Katakri I-11, ISO/IEC 27001: 12.2, Zapier "Alerts"

6.5 Second Auditing checklist for large scale IT auditing

In coordination with the assigner's requests, a second edition of the auditing checklist was formed using differing methods for checklist creation. Assigner requested a second edition of the auditing checklist comprising of larger quantity of questionnaire and the option for in-depth analysis of auditing target. Assigner suggested the use of generative artificial intelligence for the checklist compiling. So, as requested another checklist was created using artificial intelligence tools with the support of the previously created checklist. There were no restrictions given by the assigner on checklist requirements, resulting in the research including a wider range of topics researched for the auditing checklist for example physical security. As the use of artificial intelligence was suggested by the assigner, research on the tools was conducted to identify relevant choices for creating IT auditing checklists using provided sources. After reviewing various commonly used artificial intelligence tools, ChatGPT-4o and NotebookLM were chosen to create the requested IT auditing checklist.

NotebookLM (n.d.) is stated to be an artificial intelligence research assistant by Google, which breaks down documentations provided to it. It helps users take notes and understand complex topics. The tool uses only the provided materials for answering prompts from the user, as other artificial intelligence tools often use the internet for gathering information. NotebookLM said to then condense the topics or create podcasts from the presented sources making studying easier and faster. This was chosen for the research as the tool uses only the materials provided for it, so it does not alter the checklist results from external sources, or the internet compared to some alternative tools. Additionally, the software supports the use of multiple different sources.

According to *Introducing ChatGPT* (2022), ChatGPT is an trained artificial intelligence model for conversational usage. The tool is able to converse with the user and provide feedback in a dialogue. OpenAI as a company is said to be focus on making artificial intelligence that would benefit humanity (*About*, n.d.). ChatGPT-4o was used for giving feedback on the checklist compiled in NotebookLM and adjusting the compiled checklist as the tool often provided the best results in terms of overall checklist quality improvements.

The creation process comprised of gathering information on relevant checklists and auditing standards that were previously found, but not utilized for the main IT auditing checklist. The gathered material was then given to NotebookLM artificial intelligence tool for analysis as indicated in Figure 3. In addition, the AI tool was provided with the previously researched and completed main auditing checklist that had been created using cross-analysis techniques.

The main checklists and standards provided were Katakri 2020 framework, PCI-DSS checklist, NIST SP 800-53 framework, and OWASP web application checklist. Additionally, the research found relevant checklists from literature. For example, in the book "IT auditing: using controls to protect information assets" by (Kegerreis et al., 2020). They provide excellent checklists for auditing an organization ranging from policies to specific tasks, as well as tools and tutorials on how to audit specific targets. Which is why it was chosen additionally as one of the main sources for the IT auditing checklist. So, the checklist was created using various standard checklists, frameworks, guides and literature for the basis of compiling an IT auditing checklist using artificial intelligence tools. Additionally, including the main checklist created using cross analysis. List of the sources provided to NotebookLM can be found in Table 2. The book by Kegerreis et al. (2020) was used to extract Chapters 3-16 from Part 2, which contained checklists for IT auditing. These chapters were printed and supplied to the tool for processing.

Table 2 Second checklist sources

Source	Specific material
The main checklist created using cross analysis	Main checklist questions.pdf
"IT auditing: using controls to protect information assets" by (Kegerreis et al., 2020)	Part 2 Auditing Techniques: Chapters: 3 - 16
Information security auditing tool for authorities - Katakri	Katakri - 2020_1218.pdf
OWASP Penetration Testing Check List	OWASP_Web_Application_Penetration_Checklist_v1_1.pdf
PCI DSS v3.2.1 Quick Reference Guide	PCI_DSS-QRG-v3_2_1.pdf
Framework for Improving Critical Infrastructure Cybersecurity - NIST	cybersecurity-framework-021214.pdf

NotebookLM tool then created a checklist which was analyzed by ChatGPT and asked to give feedback on the list. Few iterations were created to find the sufficient candidate for further analysis and specification. ChatGPT was given prompts to verify that the list could be utilized for auditing a medium sized e-commerce organization as the research topic focused on that task. Results from the feedback were then analyzed manually and asked ChatGPT to regenerate the checklist using the adjustments provided by the feedback. The final result of the checklist was then reviewed manually and required changes were added to fit the specified use case according to the assigner.

In conclusion, the checklist was created using artificial intelligence tools by giving specific prompts in addition to providing it with sufficient source material from previous findings, as well as the main checklist created from cross analyzing the main sources. Specific prompts included asking ChatGPT to critique the checklist based on criteria required to audit a medium sized e-commerce company. The generative AI was then asked to give feedback on the usability and reliability of the checklist, and the feedback was used to improve the overall quality of the checklist. The outcome was a list comprised of twelve larger topic sections each then divided into specified requirements, targeted towards auditing a medium sized e-commerce company. Checklist can be utilized in various ways, for example replacing or adding questions to the main checklist, or using the list for

Master's degree studies. The process of leading to the finalized product is visualized in Figure 3. Results of the checklist can be found in Appendix 3.

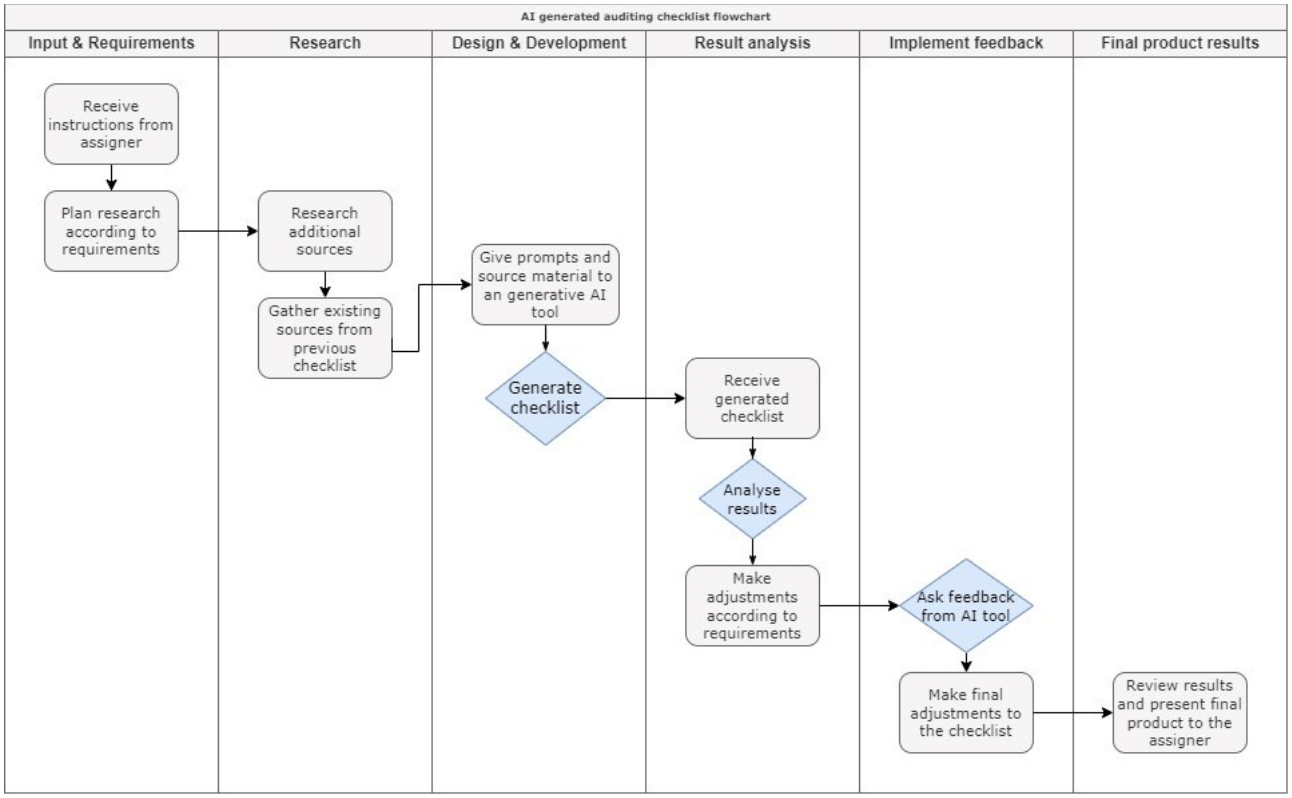

Figure 3 Second auditing checklist flowchart

7 Conclusion

The research indicates that auditing requirements are typically established by industry standard organizations, which are made up of experts from around the world in their respective fields. These organizations aim to set guidelines for companies and organizations to follow, so that they can establish a common ground for the level of requirements. Each industry often has their own standards that are strictly followed in the aims to move the industry forwards and reduce possible risks. A common practice for auditors is to use auditing checklists to perform auditing tasks faster and more efficiently.

The primary aim of this research was to develop a comprehensive IT auditing checklist to be used for the Auditing, Penetration testing and Red Teaming course taught at JAMK University of Applied Sciences. Focus was to research premade checklists from various sources and cross analyze the

similarities, which would be condensed into an IT auditing checklist for educational purposes that fit the course scope and criteria. Research aimed to create the checklist so that the teacher could utilize it for the course by analyzing the product and mend it to fit the educational criteria set by the Institute of Technology.

Research found various IT auditing checklists for different use cases, and which follow specific auditing standards. Some of the findings implicated that most auditing checklists that follow specific auditing standards, most often have multiple similarities. These similarities seemed to be caused by auditing checklist tools and standards following or referencing each other in some cases which would cause them to reflect one another. Similarities included topics around risk-management, information security, network security, cyber security programs, and several other topics, which were then used in the checklists in the development process. Research also found auditing checklists to be widely used by organizations regardless of their industry. Literature indicated them to be effective and efficient for standardizing auditing assessments limiting changes for human error. Although they were found to be reliable tools for auditing, it was told that checklists needed to be created with careful consideration and planning for each evaluation. This was found to require skills and expertise that would require organizations to have dedicated internal auditing teams as well as proper risk management procedures. While the internal teams could create purposeful checklists, external auditing specialists would still be required to evaluate organizations pursuing certification by auditing standard organizations.

Ultimately, the final product produced was a checklist consisting of 34 questions targeted towards auditing a typical organization's environment, that could be utilized on the course. While researching for the checklist, it came imminent that a larger checklist would be required for optimal usage, and as a request by the assigner, a larger checklist was produced using different methods of creating the checklist. So, in the end two checklists were produced of which the smaller one was focused to serve as a tool for the course and the larger one was to serve as possible tool for other courses or scenarios as well as to support the main checklist. The larger checklist was compiled from multiple sources in addition to the sources found for the main checklist, which were then cross-analyzed by AI tools to create a checklist. Results were then analyzed by another AI tool and finally analyzed manually, while correcting possible errors. Both lists used Open-source materials or materials available for the JAMK students through various online platforms.

The checklists should provide students with sufficient questions and topics to help understand the basics of IT auditing according to the specified course criteria. As the course criteria would probably change for future curriculums, the main checklist would need to be modified to accommodate each environment, which can be possibly done by utilizing the second checklist as supportive material. Due to the nature of auditing checklists, general purpose lists are not reliable enough to serve every environment, which is why the course teacher should alter the developed checklist for each specific use case. Research found the secondly developed checklist to be more comprehensive and better structured, thus it would be recommended to utilize the second checklist to alter the original checklist to accommodate it to suit the course structure.

7.1 Reliability and reviewing results

The research method chosen was the qualitative method, as it was seen to be to most beneficial for the research topic. Research focused on using scientific sources as well as known standard publications to conduct the checklist cross analysis. Due to the challenges of finding reliable open-source materials for all IT standards, some known publications and articles were also used to backup claims of the main sources for creating checklist questionnaire. Based on some previous knowledge on the Auditing, Penetration Testing, and Red Teaming course, understanding the course requirements were used in some aspects of developing the cross analyzed IT auditing checklist.

Research reliability could be regarded as not entirely scientific, as many areas of the research had to be developed and evaluated based on the knowledge of the researcher lacking a scientific and structured approach to the research. The limited requirements by the assigner gave the research freedom to choose criteria and checklists to follow, which inadvertently brought less reliable results from the checklist. Research chose the checklists and standards to follow based on the most commonly used open-source materials that could be found, which could be argued to be unreliable as future research could likely find different results on commonly used standards based on the point of view of the research, which would deem the research non-replicable. The second IT auditing checklist produced used AI tools to cross-analyze the data using given prompts and then the researcher evaluated the results to identify errors. This way proved to be more reliable and improved the overall quality of the checklist substantially, while creating a larger quantity of requirement and topics. This improvement could be verified based on the learned knowledge on the topic

during the research to determine the quality of the checklist compared to the original checklist, even though the findings could be regarded as opinionated due to the influence on the subject. The replicability of the second checklist would be considered better, but the evolving nature of AI tools might hinder the analysis for future iterations.

7.2 Future research ideas

Future research on this topic holds substantial potential, given the flexibility and accessibility of auditing checklists as a research area. Since this study focused on open-source materials for educational purposes, numerous avenues remain for further investigation. One possible direction could involve incorporating closed-source materials related to IT auditing standards and checklists, as many prominent standards are behind paywalls. Additionally, a tailored IT auditing checklist could be developed for specific environments with known assets and risks, aligning it with real-world scenarios where organizations seek certification from standard organizations or other credible entities.

Further, practical testing scenarios could be introduced by inviting experienced IT professionals to use the created checklists for auditing purposes and to evaluate its accuracy and usability. Interviews with auditing professionals could also provide insights into essential checklist requirements. This could also be conducted using students as evaluator during the course. So, future research could include testing the created IT auditing checklists and adapting the checklists and materials to correspond to the required needs, while fixing possible errors.

References

Abdou, M., Ezz, A. M., & Farag, I. (2021). Digital Automation Platforms Comparative Study. *2021 4th International Conference on Information and Computer Technologies (ICICT)*, 279–286. https://doi.org/10.1109/ICICT52872.2021.00052

About. (n.d.). Retrieved November 11, 2024, from https://openai.com/about/

About detection rules | Elastic. (n.d.). [Learn/Docs/Security/Guide/8.15]. Retrieved September 14, 2024, from https://www.elastic.co/guide/en/security/current/about-rules.html

About NIST. (2009). *NIST*. https://www.nist.gov/about-nist

About Us. (n.d.). *PCI Security Standards Council*. Retrieved September 29, 2024, from https://www.pcisecuritystandards.org/about_us/

About-us. (n.d.). *Sprinto*. Retrieved September 25, 2024, from https://sprinto.com/about/

Anwita. (2024, January 17). ISO 27001 Audit Checklist [Updated]. *Sprinto*. https://sprinto.com/blog/iso-27001-audit-checklist/

Auditing, Penetration Testing and Red Teaming | Curricula, JAMK. (n.d.). Retrieved October 17, 2024, from https://opetussuunnitelmat.peppi.jamk.fi/realization/45301?lang=en

Borek, A., Parlikad, A. K., Webb, J., & Woodall, P. (2013). *Total Information Risk Management: Maximizing the Value of Data and Information Assets*. Elsevier Science & Technology. http://ebookcentral.proquest.com/lib/jypoly-ebooks/detail.action?docID=1386476

Boritz, J. E., & Timoshenko, L. M. (2014). On the Use of Checklists in Auditing: A Commentary. *Current Issues in Auditing*, *8*(1), C1–C25. https://doi.org/10.2308/ciia-50741

Calder, A. (2018). *Network and Information Systems (NIS) Regulations—A Pocket Guide for Digital Service Providers*. IT Governance Ltd. http://ebookcentral.proquest.com/lib/jypoly-ebooks/detail.action?docID=5796957

Calder, A., & Williams, G. (2015). *PCI DSS: A pocket guide* (Fourth edition). IT Governance Publishing.

Cascarino, R. E. (2012). *Auditor's Guide to IT Auditing*. John Wiley & Sons, Incorporated. http://ebookcentral.proquest.com/lib/jypoly-ebooks/detail.action?docID=818101

Chai, W., & S. Gillis, A. (n.d.). *What is Active Directory (AD)?* SearchWindowsServer. Retrieved September 6, 2024, from https://www.techtarget.com/searchwindowsserver/definition/Active-Directory

Chiradeep, B. (2022, June 16). DMZ Working, Examples, Importance. *Spiceworks Inc*. https://www.spiceworks.com/it-security/network-security/articles/what-is-demilitarized-zone/

Coleman, L. B. (2015). *Advanced Quality Auditing: An Auditor's Review of Risk Management, Lean Improvement, and Data Analysis*. ASQ Quality Press. http://ebookcentral.proquest.com/lib/jypoly-ebooks/detail.action?docID=6356754

Data Obfuscation, Technique T1001—Enterprise | MITRE ATT&CK®. (n.d.). Retrieved November 8, 2024, from https://attack.mitre.org/techniques/T1001/

Educate yourself to be a Cyber Security Professional. (n.d.). JAMK University of Applied Sciences - JAMK. Retrieved October 9, 2024, from https://www.jamk.fi/en/apply-to-Jamk/masters-degree/educate-yourself-to-be-a-cyber-security-professional

End-of-life software: What are the dangers? (2016, May 4). IT Articles. https://www.spiceworks.com/it-articles/end-of-life-software-dangers/

Esheridan. (n.d.). *Blocking Brute Force Attacks | OWASP Foundation*. Retrieved November 8, 2024, from https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks

Gantz, S. D. (2013). *The Basics of IT Audit: Purposes, Processes, and Practical Information*. Elsevier Science & Technology Books. http://ebookcentral.proquest.com/lib/jypoly-ebooks/detail.action?docID=1550527

Garn, D. (2024, October 4). *How to conduct firewall testing and analyze test results | TechTarget*. https://www.techtarget.com/searchsecurity/tutorial/How-to-conduct-firewall-testing-and-analyze-test-results

Get a Master's Degree | Jamk Master School. (n.d.). JAMK University of Applied Sciences - JAMK. Retrieved October 9, 2024, from https://www.jamk.fi/en/apply-to-jamk/get-a-masters-degree-jamk-master-school

Godluck, A. (2023, July 3). Fundamental Security Postures: Default Allow vs. Default Deny. *Medium*. https://medium.com/@gakyoo/fundamental-security-postures-default-allow-vs-default-deny-539abfbbdba9

Goldman, L. (2023, March 17). Why Load Balancers Should be Part of Your Security Architecture—Spiceworks. *Spiceworks Inc*. https://www.spiceworks.com/it-security/network-security/guest-article/load-balancers-security-architecture/

Goucher, W. (2016). *Information security auditor* (1st edition). BCS, The Chartered Institute for IT.

Grassi, P. A., Fenton, J. L., Newton, E. M., Perlner, R. A., Regenscheid, A. R., Burr, W. E., Richer, J. P., Lefkovitz, N. B., Danker, J. M., Choong, Y.-Y., Greene, K. K., & Theofanos, M. F. (2017). *Digital identity guidelines: Authentication and lifecycle management* (NIST SP 800-63b; p. NIST SP 800-63b). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63b

Heiligenstein, L. (2024, April 16). *Indicator Removal: Clear Windows Event Logs, Sub-technique T1070.001—Enterprise | MITRE ATT&CK®*. https://attack.mitre.org/techniques/T1070/001/

Helgeson, J. W. (2009). *The Software Audit Guide*. ASQ Quality Press. http://ebookcentral.proquest.com/lib/jypoly-ebooks/detail.action?docID=3002613

Hingarh, V., & Ahmed, A. (2013). *Understanding and Conducting Information Systems Auditing*. John Wiley & Sons, Incorporated. http://ebookcentral.proquest.com/lib/jypoly-ebooks/detail.action?docID=1120865

Home | Curricula, JAMK. (n.d.). Retrieved October 7, 2024, from https://opetussuunnitelmat.peppi.jamk.fi/fi/48/fi/5290

IBM Security Randori. (2024, May 10). https://www.ibm.com/docs/en/randori?topic=guidance-high-risk-port

Information security auditing tool for authorities – Katakri. (2020). Ministry for Foreign Affairs. https://um.fi/information-security-auditing-tool-for-authorities-katakri

Introducing ChatGPT. (2022, November 30). https://openai.com/index/chatgpt/

IP Spoofing & Spoof Attacks. (2018, January 12). Kaspersky. https://www.kaspersky.com/resource-center/threats/ip-spoofing

IPS. vs. IDS vs. Firewall: What Are the Differences? (n.d.). Palo Alto Networks. Retrieved September 12, 2024, from https://www.paloaltonetworks.com/cyberpedia/firewall-vs-ids-vs-ips

Isaca, Isaca, & Information Systems Audit and Control Association (Eds.). (2014). *Implementing the NIST Cybersecurity Framework*. Information Systems Audit and Control Association.

ISO - About ISO. (n.d.). ISO. Retrieved October 6, 2024, from https://www.iso.org/about

ISO - International Organization for Standardization. (2024, September 12). ISO. https://www.iso.org/home.html

ISO - ISO/IEC 27000 family—Information security management. (2022, October 25). ISO. https://www.iso.org/standard/iso-iec-27000-family

ISO 27001:2013 – Annex A.10: Cryptography | ISMS.online. (n.d.). Https://Www.Isms.Online/. Retrieved September 13, 2024, from https://www.isms.online/iso-27001/annex-a-10-cryptography/

ISO 27001:2022 Annex A Control 8.30—What's New? | ISMS.online. (n.d.). Https://Www.Isms.Online/. Retrieved September 13, 2024, from https://www.isms.online/iso-27001/annex-a/8-30-outsourced-development-2022/

IT-instituutti. (n.d.). Jyväskylän ammattikorkeakoulu - JAMK. Retrieved October 9, 2024, from https://www.jamk.fi/fi/jamk/organisaatio/teknologiayksikko/it-instituutti

IT-standardoinnin vuosiseminaari. (2023, November 30). SFS. https://sfs.fi/it-standardoinnin-vuosiseminaari-2023/

Johannesson, P., & Perjons, E. (2014). *An Introduction to Design Science* (1st ed. 2014). Springer International Publishing : Imprint: Springer. https://doi.org/10.1007/978-3-319-10632-8

Kegerreis, M., Schiller, M., Davis, C., & Wrozek, B. (2020). *IT auditing: Using controls to protect information assets* (Third edition). McGraw-Hill Education.

Key Firewall Best Practices. (n.d.). Palo Alto Networks. Retrieved September 11, 2024, from https://www.paloaltonetworks.com/cyberpedia/firewall-best-practices

Kosinski, M., & Forrest, A. (2023, December 15). *What is Vulnerability Scanning? | IBM*. https://www.ibm.com/topics/vulnerability-scanning

Laadullinen tutkimus. (n.d.). Retrieved November 6, 2024, from https://sites.app.jyu.fi/mehu/fi/menetelmapolku/tutkimusstrategiat/laadullinen-tutkimus

LabraNet – Study Network. (n.d.). Retrieved November 14, 2024, from https://student.labranet.jamk.fi/

Lake, J. (2019, February 25). What is TLS encryption and how does it work? *Comparitech*. https://www.comparitech.com/blog/information-security/tls-encryption/

MBA, J. F. (2024, February 26). *How Often Should You Perform A Network Vulnerability Scan?* PurpleSec. https://purplesec.us/learn/how-often-perform-vulnerability-scan/

Merhout, J. W., & Havelka, D. (2008). Information Technology Auditing: A Value-Added IT Governance Partnership between IT Management and Audit. *Communications of the Association for Information Systems*, *23*. https://doi.org/10.17705/1CAIS.02326

Moeller, R. R. (2010). *IT Audit, Control, and Security*. John Wiley & Sons, Incorporated. http://ebookcentral.proquest.com/lib/jypoly-ebooks/detail.action?docID=624573

Network Segmentation Using Zones. (2024, August 21). https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/zone-protection-and-dos-protection/network-segmentation-using-zones

NIST - Framework for Improving Critical Infrastructure Cybersecurity. (2014). https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf

NotebookLM | Note Taking & Research Assistant Powered by AI. (n.d.). Retrieved November 11, 2024, from https://notebooklm.google/

Ohje erillistyöasemien tietoturvallisuuden varmistamisesta. (2023, October 25). Kyberturvallisuuskeskus. https://www.kyberturvallisuuskeskus.fi/fi/saadokset/ohje-erillistyoasemien-tietoturvallisuuden-varmistamisesta

Pompon, R. (2016). *IT Security Risk Control Management: An Audit Preparation Plan* (1st ed. 2016) [Electronic resource]. Apress : Imprint: Apress. https://doi.org/10.1007/978-1-4842-2140-2

PowerShell Detections. (2021, September 7). Splunk. https://www.splunk.com/en_us/blog/security/powershell-detections-threat-research-release-august-2021.html

Require Strong Passwords | CISA. (n.d.). Retrieved November 8, 2024, from https://www.cisa.gov/secure-our-world/require-strong-passwords

Saaranen-Kauppinen, A., & Puusniekka, A. (2006). *Mitä laadullinen tutkimus on: Lyhyt oppimäärä*. https://www.fsd.tuni.fi/menetelmaopetus/kvali/L1_2.html

Scarfone, K., & Hoffman, P. (2009). *Guidelines on Firewalls and Firewall Policy* (NIST Special Publication (SP) 800-41 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-41r1

School of Technology. (n.d.). JAMK University of Applied Sciences - JAMK. Retrieved October 17, 2024, from https://www.jamk.fi/en/jamk/organisation/school-of-technology

Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication (SP) 800-53 Rev. 5). (2020). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5

Security log management and logging best practices | TechTarget. (n.d.). Security. Retrieved September 13, 2024, from https://www.techtarget.com/searchsecurity/tip/Security-log-management-and-logging-best-practices

Shaoolian, G. (2021, October 4). *Elevator Inspection Checklist: 19 Essential Checklist Items*. doForms. https://www.doforms.com/elevator-maintenance-checklist/

Sharron, M. (2023, December 14). *ISO 27001 Requirement 7.5 – Documented Information | ISMS.online*. Https://Www.Isms.Online/. https://www.isms.online/iso-27001/documented-information/

Sheldon, R. (2024, February). *What is Encryption and How Does it Work? | Definition from TechTarget*. https://www.techtarget.com/searchsecurity/definition/encryption

Showcase – Virtual Learning Environment. (n.d.). Retrieved October 10, 2024, from https://index.vle.fi/showcase/

Speed, T. J. (2012). *Asset protection through security awareness* (1st edition). CRC Press. https://doi.org/10.1201/b11355

Stone, M., Irrechukwu, C., Perper, H., Wynne, D., & Kauffman, L. (2018). *IT asset management: Financial services* (NIST SP 1800-5; p. NIST SP 1800-5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.1800-5

The Role of Internal Auditing in Enterprise-wide Risk Management. (2009, January). The IIA. https://www.theiia.org/en/content/position-papers/2009/the-role-of-internal-auditing-in-enterprise-wide-risk-management/

Understanding Anti-Virus Software | CISA. (2009, June 30). https://www.cisa.gov/news-events/news/understanding-anti-virus-software

Vacca, J. R. (2009). *Computer and Information Security Handbook*. Elsevier Science & Technology. http://ebookcentral.proquest.com/lib/jypoly-ebooks/detail.action?docID=453166

Vacca, J. R. (2017). *Computer and information security handbook* (Third edition). Morgan Kaufmann Publishers. http://ebookcentral.proquest.com/lib/jypoly-ebooks/detail.action?docID=4858374

Vicente, V. (2024, February 15). *Risk Assessment Matrix: Overview and Guide*. AuditBoard. https://www.auditboard.com/blog/what-is-a-risk-assessment-matrix

Virtual Learning Environment. (n.d.). Retrieved April 15, 2024, from https://index.vle.fi/

What Is a Denial of Service (DoS) Attack? (n.d.). Palo Alto Networks. Retrieved November 14, 2024, from https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos

What Is a DMZ Network and Why Would You Use It? (n.d.). Fortinet. Retrieved September 5, 2024, from https://www.fortinet.com/resources/cyberglossary/what-is-dmz

What Is a Host-Based Firewall? (n.d.). Palo Alto Networks. Retrieved September 11, 2024, from https://www.paloaltonetworks.com/cyberpedia/what-is-a-host-based-firewall

What is Agent Based Monitoring? | Key Components and Benefits. (n.d.). *Motadata*. Retrieved November 8, 2024, from https://www.motadata.com/it-glossary/agent-based-monitoring/

What is an Intrusion Detection System (IDS)? | IBM. (2023, April 19). https://www.ibm.com/topics/intrusion-detection-system

What Is Continuous Monitoring? - CrowdStrike. (n.d.). Crowdstrike.Com. Retrieved September 13, 2024, from https://www.crowdstrike.com/cybersecurity-101/observability/continuous-monitoring/

What is Firewall Configuration and Why is it Important? (n.d.). Fortinet. Retrieved November 7, 2024, from https://www.fortinet.com/resources/cyberglossary/firewall-configuration

What Is Information Security? (n.d.). Fortinet. Retrieved October 31, 2024, from https://www.fortinet.com/resources/cyberglossary/information-security

What Is Information Security? | IBM. (2023, July 26). https://www.ibm.com/topics/information-security

What Is Network Segmentation? (n.d.). Cisco. Retrieved November 8, 2024, from https://www.cisco.com/c/en/us/products/security/what-is-network-segmentation.html

What is Principle of Least Privilege (POLP)? - CrowdStrike. (n.d.). Crowdstrike.Com. Retrieved September 13, 2024, from https://www.crowdstrike.com/cybersecurity-101/principle-of-least-privilege-polp/

What is SIEM? How does it work? (n.d.). Fortinet. Retrieved November 8, 2024, from https://www.fortinet.com/resources/cyberglossary/what-is-siem

What is SSL (Secure Sockets Layer)? (n.d.). Retrieved November 14, 2024, from https://www.cloudflare.com/learning/ssl/what-is-ssl/

What Is the OSI Model? | IBM. (2024, June 11). https://www.ibm.com/think/topics/osi-model

What Is the Principle of Least Privilege? (n.d.). Palo Alto Networks. Retrieved September 6, 2024, from https://www.paloaltonetworks.com/cyberpedia/what-is-the-principle-of-least-privilege

White, M. (2024, November 5). *NIS2, passwords, and MFA: Everything you need to know*. Specops Software. https://specopssoft.com/blog/nis2-password-security-mfa/

Who we are. (n.d.). Retrieved October 6, 2024, from https://iec.ch/who-we-are

Wolke, T. (2017). *Risk management* (1st ed). De Gruyter Oldenbourg. https://doi.org/10.1515/9783110440539

Wright, C., Freedman, B., & Liu, D. (2008). *The IT regulatory and standards compliance handbook* (1st edition). Syngress Pub.

Wright, G., Ferguson, K., & Slattery, T. (n.d.). *What is a subnet (subnetwork)? | Definition from TechTarget*. Networking. Retrieved September 6, 2024, from https://www.techtarget.com/searchnetworking/definition/subnet

Appendices

Appendix 1. Risk matrix example

	Probability				
Impact	Rare (1)	Unlikely (2)	Possible (3)	Likely (4)	Certain (5)
Insignificant (1)	1	2	3	4	5
Minor (2)	2	4	6	8	10
Moderate (3)	3	6	9	12	15
Major (4)	4	8	12	16	20
Critical (5)	5	10	15	20	25

Asset	Threat/Risk	Probability	Impact	Risk Level	Mitigation Method	If escalated, Plan A
FlareVM	Attacker sends user phishing attachments via email and get control of the system.	3	4	12	Enable firewall and educate employees of phishing attacks.	Isolate machine from network and inform police if necessary.
Wasdat	Brute Force attack against Wasdat using ssh.	4	5	20	Change default credentials. Create backups for Juice Shop and Wasdat.	Isolate machine and begin forensics
PfSense	OpenSSH vulnerability allows attacker to overwrite SCP directory files	2	3	6	Establish backups and update OpenSSH version	Recover lost data from backups

FlareVM	Attacker captures data because system is using weak cipher suite.	2	4	8	Remove weak cipher suites from registry	Try to figure out what data has been captured in a MITM
FlareVM	Attacker gains access to system and has administrator rights	5	5	25	Change default credentials and remove unnecessary rights from user	Try to remove foothold of the attacker and isolate the system
Wasdat	Attacker uses vulnerable OpenSSL to crash applications to result in a DOS attack	3	5	15	Update OS version as well as update tools to latest versions. Enable firewall	Try to mitigate issue by restarting systems and updating OS.

Appendix 2. The main IT auditing checklist using cross-analysis

Network auditing

Q1.1: Is the environment's network architecture secure? Yes ☐ No ☐ N/A ☐

Describe network security measures or gaps.

Q1.2: Has the network been segmented and documented accordingly? Yes ☐ No ☐ N/A ☐

Summarize segmentation and documentation quality.

Q1.3: Does the documentation match the actual environment? Yes ☐ No ☐ N/A ☐

Describe discrepancies or confirm alignment.

Q1.4: Are there set limitations on network visibility using network segmentation? Yes ☐ No ☐ N/A ☐

Detail network visibility limitations or lack thereof.

Q1.5: Have the subnetworks been established according to the documentation? Yes ☐ No ☐ N/A ☐

Describe subnetwork setup accuracy.

Q1.6: Does the data traffic flow correctly between subnetworks? Yes ☐ No ☐ N/A ☐

Summarize traffic flow findings.

Q1.7: Has the management network been configured using Principle of Least Privileges? Yes ☐ No ☐ N/A ☐

List privileges granted or note misconfigurations.

Q1.8: Does the environment use https, TLS algorithm and other industry standards for encryption? Yes ☐ No ☐ N/A ☐

Describe encryption standards used.

Q1.9: Are there measures put in place to defend against common network attacks (Dos, Ddos, etc.)? Yes ☐ No ☐ N/A ☐

List defensive measures or gaps.

Firewall auditing

Q2.1: Does the network have firewalls and are they enabled? Yes ☐ No ☐ N/A ☐

Describe firewall presence and status.

Q2.2: Are environment's firewalls up to date? Yes ☐ No ☐ N/A ☐

Confirm updates or note any outdated versions.

Q2.3: Does the firewall/s restrict unnecessary traffic and permit only authorized traffic? Yes ☐ No ☐ N/A ☐

Summarize traffic restriction policies.

Q2.4: Has the firewall security including rules, policies, protocols and filters been tested? Yes ☐ No ☐ N/A ☐

Document testing results or gaps.

Q2.5: Has the firewall rule "deny-by-default" been enabled? Yes ☐ No ☐ N/A ☐

Confirm or document any exceptions.

Q2.6: Have the appropriate filtering policies been configured in the firewalls? Yes ☐ No ☐ N/A ☐

Describe filtering policies.

Q2.7: Are there unnecessary firewall rules, policies, filters enabled? Yes ☐ No ☐ N/A ☐

List any unnecessary rules.

Q2.8: Has the anti-virus software been deployed and updated to the latest stable version on all systems (workstations, servers etc.)? Yes ☐ No ☐ N/A ☐

Document anti-virus deployment status.

Policies and systems auditing

Q3.1: Are the assets and functionalities of the systems aligned with their intended purposes? Yes ☐ No ☐ N/A ☐

Describe alignment or misalignments.

Q3.2: Does the environments existing documentation include policies and procedures for governing risk management? Yes ☐ No ☐ N/A ☐

Summarize risk management documentation.

Q3.3: Has a risk matrix been developed for each identified risk factor? Have these risks been evaluated, and are there mitigation plans in place? Yes ☐ No ☐ N/A ☐

Create a risk matrix. Describe risk evaluation and mitigation status.

Q3.4: Have the devices and systems been scanned for vulnerabilities, and are regular environmental scans in place (e.g., using Greenbone, Nessus, Lynis)? Yes ☐ No ☐ N/A ☐

List scan tools and document performed scans on (network, firewall, web applications, servers, other devices etc.)

Information security

Q4.1: Do the systems/machines lock after a specified number of invalid login attempts? Yes ☐ No ☐ N/A ☐

Describe lockout settings or lack thereof.

Q4.2: Do password policies mandate the inclusion of alphabetic, numeric, and symbolic characters? Yes ☐ No ☐ N/A ☐

Summarize password policy requirements.

Q4.3: Do the devices satisfy the hardware requirements necessary for the programs in use? Yes ☐ No ☐ N/A ☐

Describe hardware adequacy or identify limitations.

Q4.4: Has IP address spoofing (replication/faking) been addressed? Yes ☐ No ☐ N/A ☐

List anti-spoofing measures or gaps.

Q4.5: Have the configurations and other critical assets been properly backed up and secured? Yes ☐ No ☐ N/A ☐

Confirm backup protocols or note gaps.

Q4.6: Are monitoring programs enabled and configured to generate alerts and warnings from suspicious activity? Yes ☐ No ☐ N/A ☐

List monitoring tools and alert settings.

Q4.7: Is end-to-end encryption in place to protect against intrusions? Yes ☐ No ☐ N/A ☐

Describe encryption measures.

Q4.8: Does the environment utilize continuous monitoring programs for example SIEM tools? Yes ☐ No ☐ N/A ☐

List continuous monitoring tools or note absence.

Q4.9: Have the appropriate admin privileges been provided to users using PoLP? Yes ☐ No ☐ N/A ☐

Describe privilege management practices.

Q4.2.1: Are the logs are securely stored in ways that prevent tampering? Yes ☐ No ☐ N/A ☐

Summarize logging security.

Q4.2.2: Are system logs and other critical logs regularly reviewed for abnormal behavior? Yes ☐ No ☐ N/A ☐

Document log review frequency and latest findings.

Q4.2.3: Are critical logs being monitored using program agents or similar tools? Yes ☐ No ☐ N/A ☐

List log monitoring tools/services used.

Q4.2.4: Is change detection active and functioning correctly, including file integrity monitoring and alerting users of unauthorized file modifications? Yes ☐ No ☐ N/A ☐

Describe change detection measures.

Appendix 3. The second IT auditing checklist using generative AI tools

Category	Audit item	Description	Compliance	Document findings
1. Cybersecurity Governance and Program Structure	**IT Organizational Structure**	Review IT structure for clear assignment of authority, responsibility, and segregation of duties.	Yes ☐ No ☐ N/A ☐	
	Strategic Alignment	Ensure IT strategic planning aligns with business strategies, and assess metrics for tracking performance.	Yes ☐ No ☐ N/A ☐	
	Cybersecurity Program Oversight	Evaluate the structure of the company's cybersecurity program, ensuring policies and oversight mechanisms are in place.	Yes ☐ No ☐ N/A ☐	

	Policy Review and Updates	Ensure cybersecurity policies are reviewed and updated annually to reflect changes in the threat landscape and compliance requirements.	Yes ☐ No ☐ N/A ☐	
	Risk Assessment	Review the risk-assessment processes to ensure risks are identified, evaluated, and documented, with mitigation plans tracked for completion.	Yes ☐ No ☐ N/A ☐	
	Performance Metrics	Evaluate the collection and analysis of cybersecurity performance metrics to support continuous improvement.	Yes ☐ No ☐ N/A ☐	
	Controls for Endpoint Detection and Response (EDR)	Ensure controls for endpoint detection and response (EDR) are implemented, including regular validation of EDR effectiveness.	Yes ☐ No ☐ N/A ☐	
2. Identity and Access Management (IAM)	**User Account Management**	For Windows servers, ensure accounts are managed at the domain level, documented in Active Directory, and traceable to specific users.	Yes ☐ No ☐ N/A ☐	

		For Unix/Linux systems, confirm: • Unique user IDs and shadowed passwords with strong hashes. • Appropriate permissions on password files and invalid shells on disabled accounts.	Yes ☐ No ☐ N/A ☐	
		Verify user account creation processes are restricted to necessary personnel, with clear procedures for removal upon role change or termination.	Yes ☐ No ☐ N/A ☐	
		Confirm all user accounts, especially for administrative access, are unique and documented in a centralized IAM system.	Yes ☐ No ☐ N/A ☐	
	Password Policies	Ensure that password policies enforce complexity, aging, and history requirements, and that account lockout policies are configured.	Yes ☐ No ☐ N/A ☐	

	Access Control Reviews	Conduct periodic reviews of user rights and access to sensitive systems, following the Principle of Least Privilege (PoLP).	Yes ☐ No ☐ N/A ☐	
	Multi-Factor Authentication (MFA)	Require MFA for accessing sensitive systems and for high-risk actions, including payment processing and data exports.	Yes ☐ No ☐ N/A ☐	
3. Network Security and Firewall Auditing	**Network Architecture and Segmentation**	Ensure the network architecture has secure segmentation, with separate zones for sensitive, intranet, and external systems.	Yes ☐ No ☐ N/A ☐	
	Firewall Configuration and Rules	Confirm that firewalls are configured with a deny-by-default policy, only allowing documented, necessary traffic. Regularly review and test firewall rules for redundancies and effectiveness.	Yes ☐ No ☐ N/A ☐	
		Ensure application-layer protections (Layer 7) are configured on firewalls for HTTP/S and FTP traffic to filter malicious activities.	Yes ☐ No ☐ N/A ☐	
	Firewall Software Updates and Testing	Verify that firewall software is regularly updated and that configurations are tested to ensure rule functionality.	Yes ☐ No ☐ N/A ☐	

	Real-Time Network Monitoring	Implement real-time network traffic monitoring and alerts for unusual patterns, including potential intrusions and DDoS attacks.	Yes ☐ No ☐ N/A ☐	
	Network Services and Protocols	Disable unnecessary network services (e.g., FTP, NFS) and enforce secure protocols (e.g., HTTPS, TLS).	Yes ☐ No ☐ N/A ☐	
		Secure SSH access by limiting trusted access via keys, logging activity, and ensuring encrypted sessions.	Yes ☐ No ☐ N/A ☐	
	Wireless Network Security	Ensure that access points use strong encryption, are managed centrally, and are regularly scanned for rogue devices.	Yes ☐ No ☐ N/A ☐	
4. Policies and Systems Auditing	**System Alignment**	Review system assets and ensure functionalities align with business objectives.	Yes ☐ No ☐ N/A ☐	
	Risk Documentation	Confirm that a risk matrix exists, is up-to-date, and includes documented remediation plans for identified risks.	Yes ☐ No ☐ N/A ☐	
	BCP Development and Testing	Develop a business continuity plan tailored to organizational needs. Regularly test	Yes ☐ No ☐ N/A ☐	

		BCP to ensure critical operations can continue during disruptions.		
	Vulnerability Scanning	Ensure regular vulnerability scans cover all systems, with high-priority issues tracked and addressed promptly.	Yes ☐ No ☐ N/A ☐	
	Approved Applications and Scheduled Tasks	Only approved applications and scheduled tasks should run on servers. Review crontabs and scheduled tasks for any anomalies.	Yes ☐ No ☐ N/A ☐	
	System Configuration Baseline	Establish a baseline security configuration for all new systems. Periodically audit newly deployed systems to confirm baseline adherence.	Yes ☐ No ☐ N/A ☐	
5. Data Security and Privacy	**Data Loss Prevention (DLP)**	Confirm that DLP measures are implemented, with controls aligned to prevent unauthorized data exfiltration.	Yes ☐ No ☐ N/A ☐	
	Encryption	Verify that sensitive data is encrypted both at rest and in transit, using standards such as AES-256 for storage and TLS 1.2+ for transmission.	Yes ☐ No ☐ N/A ☐	
		Implement secure key management, including regular key rotation and access restrictions.	Yes ☐ No ☐ N/A ☐	
	Backup and Recovery	Regularly back up critical data and store it in secure	Yes ☐ No ☐ N/A ☐	

		offsite locations. Confirm recovery processes are tested periodically.		
	Monitoring and Alerts	Ensure continuous monitoring and alerting are configured to detect suspicious access or modifications to data.	Yes ☐ No ☐ N/A ☐	
		Establish procedures for notifying affected customers and regulatory bodies in case of a data breach, in line with GDPR, and PCI DSS etc.	Yes ☐ No ☐ N/A ☐	
	Data Privacy Compliance	Review data handling processes to confirm compliance with relevant privacy regulations (e.g., GDPR), including data retention and secure disposal practices.	Yes ☐ No ☐ N/A ☐	
	Data Ownership and Classification	Define data ownership, classify data based on sensitivity, and establish retention and lifecycle policies.	Yes ☐ No ☐ N/A ☐	
	Data Segregation and Access Control	Ensure sensitive customer data is segregated and access-controlled within systems.	Yes ☐ No ☐ N/A ☐	
6. E-Commerce and PCI DSS Compliance	**PCI DSS Controls**	Ensure that all systems handling payment data meet PCI DSS standards, including access control, logging, and encryption requirements.	Yes ☐ No ☐ N/A ☐	

	HTTPS Enforcement	Confirm HTTPS is enforced on all customer-facing pages, especially for login, checkout, and data entry forms.	Yes ☐ No ☐ N/A ☐	
	Employee Training on Compliance	Provide training for employees handling payment data on PCI DSS requirements and secure data handling practices.	Yes ☐ No ☐ N/A ☐	
7. Web Application Security	**OWASP Top 10**	Assess web applications for vulnerabilities in alignment with the OWASP Top 10, including SQL injection, XSS, and CSRF.	Yes ☐ No ☐ N/A ☐	
	Web Application Firewall (WAF)	Ensure a WAF is deployed to block malicious web traffic and protect against application-layer attacks.	Yes ☐ No ☐ N/A ☐	
	Access Control for Web Servers	Enforce least privilege for web server accounts and restrict access where necessary.	Yes ☐ No ☐ N/A ☐	
	Session Management	Verify secure session management practices, including session expiration and secure cookie handling.	Yes ☐ No ☐ N/A ☐	
	Input Validation	Confirm that input validation is enforced to prevent injection attacks and unauthorized commands.	Yes ☐ No ☐ N/A ☐	
	Fraud Detection and	Use real-time fraud detection tools to monitor for	Yes ☐ No ☐ N/A ☐	

	User Behavior Analytics	suspicious activities, including unusual login patterns or rapid payment failures.		
8. Cloud Security Controls	**Cloud Infrastructure Security**	Confirm cloud infrastructure has access controls, encryption, and monitoring aligned with company policies.	Yes ☐ No ☐ N/A ☐	
	Data Retention and Destruction for Cloud Services	Ensure cloud service providers follow data retention and secure destruction policies in compliance with company policies.	Yes ☐ No ☐ N/A ☐	
	API Security	Ensure third-party APIs use strong authentication, encryption, and rate-limiting to prevent abuse and data leakage.	Yes ☐ No ☐ N/A ☐	
	Vendor Agreements and Compliance	Review vendor agreements to ensure alignment with internal security requirements, including data retention and secure disposal.	Yes ☐ No ☐ N/A ☐	
	Offsite Data Storage	Ensure offsite data storage at vendor locations meets internal security policies and is regularly audited for compliance.	Yes ☐ No ☐ N/A ☐	
	Incident Notification from Vendors	Confirm that vendors are contractually required to notify your organization of security breaches immediately and to provide support for investigations.	Yes ☐ No ☐ N/A ☐	

9. Incident Response and Breach Management	**Incident Response Plan Testing**	Test the incident response plan regularly, with simulations for data breaches and customer notifications.	Yes ☐ No ☐ N/A ☐	
	Breach Notification	Ensure documented breach notification processes are in place, with defined roles for regulatory and customer communication.	Yes ☐ No ☐ N/A ☐	
	Response Protocols	Verify that procedures for real-time alerting and escalation are in place and actively monitored by the security operations center (SOC).	Yes ☐ No ☐ N/A ☐	
	Post-Incident Analysis	After incidents, conduct root cause analysis and update policies and procedures to prevent recurrence.	Yes ☐ No ☐ N/A ☐	
	SIEM Integration	Use a SIEM to centralize log collection from critical systems, supporting real-time monitoring and alerting.	Yes ☐ No ☐ N/A ☐	
	Alert Configuration	Configure automated alerts for high-risk events, including unauthorized access attempts, failed logins, and data exports.	Yes ☐ No ☐ N/A ☐	

10. Third-Party Vendor Management	**Vendor Risk Assessment**	Conduct regular risk assessments for critical vendors, focusing on security controls, data handling, and incident response capabilities.	Yes ☐ No ☐ N/A ☐	
	Contractual Requirements	Ensure contracts specify security requirements, including breach notification timelines and compliance with privacy regulations.	Yes ☐ No ☐ N/A ☐	
11. Endpoint and System Hardening	**Windows Servers**	Confirm firewalls, anti-virus, and patch management solutions are enabled on all Windows servers.	Yes ☐ No ☐ N/A ☐	
		Review and enforce group policies for password complexity, access controls, and logging.	Yes ☐ No ☐ N/A ☐	
	Unix/Linux Hosts	Verify user accounts follow PoLP, and that privileged access is restricted and monitored.	Yes ☐ No ☐ N/A ☐	
		Ensure SSH configurations are secure, with access limited to necessary personnel.	Yes ☐ No ☐ N/A ☐	
		Confirm logs are retained securely and reviewed regularly, with appropriate retention policies.	Yes ☐ No ☐ N/A ☐	
	Web Servers	Ensure web servers are dedicated, fully patched, and hardened to minimize unnecessary services.	Yes ☐ No ☐ N/A ☐	

	Web Applications	Verify secure coding practices and session security for web applications.	Yes ☐ No ☐ N/A ☐	
		Review error handling processes to ensure that sensitive information is not exposed to end-users.	Yes ☐ No ☐ N/A ☐	
	Databases	Verify that database systems are patched, encrypted, and meet access control policies.	Yes ☐ No ☐ N/A ☐	
		Ensure activity monitoring is enabled, with alerts for suspicious database actions.	Yes ☐ No ☐ N/A ☐	
12. Continuous Improvement and Security Training	**Policy and Process Review**	Conduct an annual review of all policies and adjust based on lessons learned from past incidents and updates in regulatory requirements.	Yes ☐ No ☐ N/A ☐	
	Security Awareness and Training	Provide ongoing security awareness training to all employees, emphasizing phishing prevention, secure handling of customer data, and incident reporting.	Yes ☐ No ☐ N/A ☐	
	Metrics and Continuous Improvement	Collect and analyze metrics on security performance, vulnerabilities, incident response, and policy adherence to continually improve the cybersecurity program.	Yes ☐ No ☐ N/A ☐	