UNIVERISTY OF PIRAEUS - DEPARTMENT OF INFORMATICS

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ – ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

MSc «Cybersecurity and Data Science»

ΠΜΣ «Κυβερνοασφάλεια και Επιστήμη Δεδομένων»

MSc Thesis

Μεταπτυχιακή Διατριβή

Thesis Title: Τίτλος Διατριβής:	**Cybersecurity standards in the certification of digital products** Πρότυπα κυβερνοασφάλειας στην πιστοποίηση ψηφιακών προϊόντων
Student's name-surname: Ονοματεπώνυμο φοιτητή:	**Dimopoulos Karolos** Δημόπουλος Κάρολος
Father's name: Πατρώνυμο:	**Ioannis** Ιωάννης
Student's ID No: Αριθμός Μητρώου:	ΜΠΚΕΔ21012
Supervisor: Επιβλέπων:	**Despina Polemi, Professor** Δέσποινα Πολέμη, Καθηγήτρια

September 2024/ Σεπτέμβριος 2024

3-Member Examination Committee

Τριμελής Εξεταστική Επιτροπή

Despina Polemi **Professor**	**Christos Douligeris** **Professor**	**Panayiotis Kotzanikolaou** **Professor**
Δέσποινα Πολέμη Καθηγήτρια	Χρήστος Δουληγέρης Καθηγητής	Παναγιώτης Κοτζανικολάου Καθηγητής

Acknowledgements

I would like to express my gratitude to my supervisor, Professor Despina Polemi for her guidance, help and patience during the whole project. I would also like to thank my family and friends for their support.

Abstract

This thesis explores the role of cybersecurity standards in the certification of digital products, focusing on the implementation of international standards like ISO/IEC 15408, ISO/IEC 18045, and the updated ISO/IEC 27001:2022. It examines key regulations such as the European Cybersecurity Act, the Cyber Resilience Act, and the NIS2 Directive, which guide certification processes to ensure security and reliability in digital infrastructures. By analyzing the impact of emerging technologies such as AI and cloud services, the research highlights the challenges these technologies pose to cybersecurity frameworks. A case study involving a company providing digital products is presented, where an external audit is conducted to assess the practical application of ISO/IEC 27001:2022. This audit underscores the critical vulnerabilities that arise during compliance and the necessity for adaptable cybersecurity measures in an evolving technological landscape. The thesis concludes by suggesting that future cybersecurity efforts should focus on integrating AI, blockchain, and other emerging technologies into certification processes to enhance the overall security and resilience of digital products.

Contents

1. Introduction

1.1 Fundamentals of Cybersecurity

Digital industries of today face the challenge of establishing robust cybersecurity certification. So is it for sectors witnessing a growing level of digitalization, therefore it is important to ensure that their important digital infrastructures are protected. The cybersecurity certification is highly essential to accomplish the security of the varied digital platforms and services. Such certifications are the indispensable guarantee of the ability to provide education to professionals in the most proper way of dealing with the potential cyber threats and thereby offering effective protection of vital digital services and cloud infrastructures. (D. P. F. Möller, 2022)

The world today is much more complicated than before. In addition, the diversity of modern technologies in information and communication makes the establishment of an exhaustive certification framework even more complex. They must adapt to the diversity of digital elements that support any range of issue types, from products to services and even to complex processes. Thus, the efficient sharing and evaluation of the produced cybersecurity data through innovative technical solutions and strategic planning will assure continuous protection and robustness of the ICT systems during their operational span. (al., 2020)

The emergence of the Internet of Things (IoT) adds further intricacies to the cybersecurity certification terrain. Crafting a strong and flexible certification framework for IoT calls for a comprehensive strategy that blends various aspects. This approach should integrate diverse research, technological insights, and governance strategies to effectively tackle the unique challenges presented by IoT's dynamic nature. (Sara N. Matheu, 2021)

Moreover, the trend towards automated and instantaneous cybersecurity certification processes is gaining momentum. With such approaches becoming ever more popular due to the increasing use of automated security assessment and audit tools, certification can become both more efficient and continuous. This approach ensures that the stored digital assets will always adhere to the highest standards of security according to prevailing cybersecurity requirements (S. Karagiannis, 2021). In summary, the scope of cybersecurity certification really sums up a mix of many elements, starting from policy formulation to implementation of the technological solutions.

1.2 Cybersecurity as a Critical Component in the Digital Age

Considering the present wave of digital change, cybersecurity plays an extremely important role. As electronic systems and the Internet of Things (IoT) continue to grow, cyberspace is growing, necessitating the creation of a safe digital environment free from dangers and cybercrimes. As we see advancements in areas such as cloud computing, IoT, and mobile technology, it becomes imperative to also evolve our cybersecurity approaches (A. Salih, 2021). Modern cybersecurity strategies, which include the use of artificial intelligence and machine learning, are designed to address cyber risks that know no physical or digital boundaries. (Teoh, 2021)

Furthermore, the growing reliance on digital solutions in both personal and professional settings has made cybersecurity more significant than ever. Organizations are quickly adopting new technologies and services, integrating them into their digital transformation journey. This shift places cybersecurity at the forefront of managing enterprise risks (Mtsweni, 2018). Additionally, the ever-changing landscape of data protection and privacy laws further complicates the management of cybersecurity, requiring strategies that are both adaptive and anticipatory.

1.3 Cybersecurity Standards in Digital Product Accreditation

Cybersecurity standards play a crucial role in digital product accreditation, providing structured and consistent frameworks for implementing cybersecurity measures. These standards vary from broad international guidelines to specific industry-focused protocols, required for defining best practices, ensuring compliance, and assessing the security posture of digital products. The complexity of these standards is attributed to their varied origins and applications, covering a wide range of perspectives and requirements to reflect the diverse needs of different sectors and geographical regions.

The success of cybersecurity standards greatly depends on how they are implemented in practice, the difficulties encountered in achieving compliance, and their effectiveness in enhancing cybersecurity measures. It is important to find a middle ground between implementing rigorous security protocols and encouraging innovation and user-friendliness in digital products. These standards significantly influence market trends and building confidence among users and stakeholders.

Summarily, the evolution of cybersecurity standards reflects the dynamic nature of the digital landscape, underscoring the need for continuous adaptation and integration of sector-specific requirements to enhance the security and trustworthiness of digital products and services.

1.4 National and International Efforts in Cybersecurity Certification

1.4.1 National Efforts

In the intricate tapestry of global cybersecurity, the contributions of various standard-setting bodies are necessary. In particular, the American National Standards Institute (ANSI), the British Standards Institution (BSI), and the German Institute for Standardization (DIN) stand out as the major architects in this sector, with all of them having created their independent yet related paths in cybersecurity certification.

These efforts are personified by ANSI, acting not only as a developer of national standards but also as an interchange between U.S. standards and international standards so that American practice is in line with international requirements. Such alignment will, without doubt, provide a pivotal fillip to more international trade in American products and technology. ANSI’s partnerships, especially with the ISA and the IEC, demonstrate a keen understanding of the importance of integrating cybersecurity into key sectors like manufacturing and infrastructure. Through the assimilation of ISO Guide 73 on Risk Management Terminology, and adoption of ISO 22301-2014 for Business Continuity Management, ANSI has further established itself in such a position within the global cybersecurity architecture. The standards reflect commitments of risk-aware and resilience to the cybersecurity standards, showing the broad influence of ANSI in and around global definitions relating to cybersecurity norms.

Another influential body is the UK's BSI, who, with the development of the BS 7799 standard for information security management, marked a significant milestone in cybersecurity. BSI Group published BS 7799 for the first time in 1995. The first section of BS 7799 which concerned best practices for information technology, was incorporated into ISO 17799 and was included in the ISO 27000 family five years later. BS 7799 emerged in response to the need for managing the intricate game between advancing technology and the growing security demands. This strategic vision of BSI to have its standards synchronized with global cybersecurity protocols places the British companies and their international partners on the right platform, not just for competitive success, but for adherence to levels of security required by the international highest order. Such proactive stance outfits UK-based organizations to adeptly navigate the complexities

of a global digital marketplace, which is full and overflowing with comprehensive practices around cybersecurity.

In Germany, DIN distinguishes itself with a focus on adaptive and resilient cybersecurity standards, especially relevant in the country's renowned engineering and technology sectors. This standard, in particular, the DIN EN 17640, exemplifies the forward-looking nature of DIN in presenting methods for the determination of the cybersecurity in ICT products. This standard is the pro-active approach of DIN in addressing the ever-evolving cybersecurity landscape. Further, DIN's enormous contribution to the EU 2021 Cybersecurity Strategy does reflect the commitment it has in fostering a digitally secure future for Europe. With this background, DIN becomes an important driving force for harmonization in cybersecurity requirements and a supporter of the European Commission vision toward the implementation of mandatory cybersecurity standards that can fill the existing gaps in the continent. This is crucial to follow at a time when the digital threats become more and more professional, and it is very important that coherence is kept between the respective legal acts and standards.

In conclusion, these organizations are part of a broader, global network of national organizations, each contributing significantly to cybersecurity certification. Entities like AFNOR in France, the Japanese Industrial Standards Committee (JIS) in Japan, CSA Group in Canada, and the Hellenic Organization for Standardization (ELOT) in Greece are some of the plenty of national organizations with significant impact on cybersecurity certification. Each of these national bodies brings unique perspectives and expertise, contributing to the development and enhancement of cybersecurity measures within their respective regions and industries. Furthermore, the collective efforts of these national bodies are unified and amplified through international organizations. These international entities acknowledge these efforts across borders, ensuring that cybersecurity certification is not just a regional or national endeavor but a global one.

1.4.2 International Efforts

A concerted effort by international organizations is required to properly align and integrate the multitude of national cybersecurity operations. Leading organizations that are important in this context of cybersecurity certification are the European Union Agency for Cybersecurity (ENISA) and the National Institute of Standards and Technology (NIST) of the United States. Their combined efforts guarantee a safer and more dependable digital environment by improving security measures and setting global standards for cybersecurity expertise.

NIST, the National Institute of Standards and Technology at the U.S., stands as a foundational element in the U.S. cybersecurity framework. Prime examples include the NIST Special Publication 800-30 Rev. 1, titled "Guide for Conducting Risk Assessments", which provides a detailed guide to conducting risk assessments of information systems and organizations, and guidance that is supplementary to what is provided by NIST SP 800-39 (Managing Information Security Risk: Organization, Mission, and Information System View). This publication emphasizes that risk assessments are an integral part of the risk management process and must be performed at all three tiers of the risk management hierarchy. The institute also launched theNIST Cybersecurity Framework (CSF), in 2018, which exemplifies its commitment to advancing cybersecurity. This framework provides vital guidance for organizations, outlining necessary practices for securing computer systems and networks (Calder, 2018). NIST's National Initiative for Cybersecurity Education (NICE) has also revolutionized professional training, establishing key competencies and practices in cybersecurity and thus effectively linking academic study with industry needs (Shoemaker, 2015). Moreover, NIST's impact is evident in the Department of Defense’s Cybersecurity Maturity Model Certification (CMMC), which integrates NIST standards into a comprehensive certification model, crucial for compliance within the Defense Industrial Base (V. Sundararajan, 2022).

ENISA has become a major influence in setting European cybersecurity standards. Central to the EU Cybersecurity Act, ENISA boosts Europe's ability to compete in the global cybersecurity landscape. This Act, overseen by ENISA, seeks to standardize and enhance security standards across the EU, significantly improving security for consumers and businesses (Mitrakas, 2018). Additionally, ENISA's focus on industry-specific frameworks is highlighted by its initiatives in healthcare cybersecurity certification, demonstrating its dedication to customized and in-depth security solutions (K. Hovhannisyan, 2021). This industry-focused approach ensures that various sectors have the necessary cybersecurity defenses, tailored to their specific threats and vulnerabilities. Further, the activity of ENISA goes to cover holistic risk management, a core part of maintaining sound cybersecurity. The use of its Risk Management Inventory and the development of Risk Management Frameworks has put forward useful tools and guidelines that may enable organizations to effectively carry out assessments on risks and mitigation. These encompass the development of a mechanism through which an inventory of risk and information security management systems enables organizations to tackle their security risks systematically (ENISA, 2006).

In summary, NIST and ENISA, along with some other organizations, including (ISC)², ISACA, and SANS, have cooperated to affect the global landscape of certification in cybersecurity. Among the certification offerings of (ISC)² are CISSP, SSCP, and CCSP. From ISACA, one can have CISM, CISA, CRISC. CompTIA's certifications include Security+, CySA+ (Cybersecurity Analyst), and CASP+ (Advanced Security Practitioner). GIAC offers the GIAC Security Essentials (GSEC), GIAC Certified Incident Handler (GCIH), and GIAC Penetration Tester (GPEN) certifications. CEH (Certified Ethical Hacker), CHFI (Computer Hacking Forensic Investigator), and ECSA (EC-Council Certified Security Analyst) are offered through the EC-Council. A number of certifications are offered through GIAC's partnership with the SANS Institute. ISFCE provides the CCE (Certified Computer Examiner) certification, Offensive Security provides certifications like OSCP (Offensive Security Certified Professional), OSCE (Offensive Security Certified Expert), and OSWP (Offensive Security Wireless Professional), CertNexus provides CFR (CyberSec First Responder) and CIoTSP (Certified Internet of Things Security Practitioner), and Mile2 provides CPTE (Certified Penetration Testing Engineer), CDFE (Certified Digital Forensics Examiner), and CISSO (Certified Information Systems Security Officer). IAPP provides certifications such as CIPM (Certified Information Privacy Manager), CIPP (Certified Information Privacy Professional), and CIPT (Certified Information Privacy Technologist). Cisco provides several certifications, including CCNA Security, CCNP Security, and CCIE Security. These organizations provide a host of certifications for different levels of proficiency and specialization under information security. Their individual and joint actions make up a decisive factor in forming a single, effective global response to cybersecurity challenges.

2. EU Cybersecurity related Legal Instruments

2.1 Legal Acts

2.1.1 Overview

Global legal frameworks are a significant factor in today's cybersecurity landscape. The GDPR in the European Union is a game-changer in terms of data privacy and protection laws, impacting companies around the world (A. Pawlicka, 2020). In the US, the Cybersecurity and Infrastructure Security Agency Act established CISA, addressing various cybersecurity aspects (Falco, 2021). Other frameworks include the Data Protection Act in the UK, the IT Act in India, and the Privacy Act in Australia.

The regulations are, therefore, not just compliance mechanisms but elements that seek to encourage organizations and individuals towards cyber solid defense measures, which contribute to a great extent to the global digital security paradigm.

2.1.2 The Role of Legal Acts in Shaping Cybersecurity Standards

Legal acts will influence the development of standards about cybersecurity. The global impact of the GDPR on the standards for data protection illustrates how, in compliance with legal requirements, one has to shape standards within cybersecurity (Sara Degli-Esposti, 2021). The relationship between legal laws and the technical specification of cybersecurity is complex. With the laws providing the framework under which the stated standards operate, the legislators, in this case, come up with the reference points in cyber risk management. At the same time, they also have challenges that need harmonious integration of legal and technical requirements. This relationship is best demonstrated when the standards have been aligned to the legal delegation, such as the NIST framework from the United States. Both show their relationship to each other for synergy between legal compliance and the relationship of NIS regulations.

2.1.3 Legal Requirements and Digital Product Cybersecurity Certification

Legal requirements significantly influence the certification of digital products, affecting various aspects of the process. These regulations shape the criteria, procedures, and outcomes of certifying digital products (Dimitra Markopoulou, 2019).

Throughout the certification process, integrating legal compliance seamlessly is crucial to ensure that digital products rigorously conform to relevant laws and regulations. This integration impacts the entire lifecycle of digital products, from conception and development to evaluation (K. Hovhannisyan, 2021). Legal mandates provide a direct blueprint for the standards and guidelines used in certifying products, especially those handling sensitive data or operating in critical infrastructure (Kohler, 2020).

Real-world examples, such as products subject to the GDPR or those designed for regulated sectors like finance or healthcare, illustrate the direct impact of legal requirements on product certification (Najmudin Saqib, 2020). These examples demonstrate the comprehensive spectrum of challenges and opportunities faced by organizations in complying with these requirements.

Compliance demands rigorous effort and meticulous attention to detail. However, adherence to legal mandates simultaneously enhances the security and reliability of digital products. In essence, legal requirements play an indispensable role in continually improving cybersecurity standards for digital products.

2.2 European Cybersecurity Act

2.2.1 Overview

A major legislative achievement in the European Union's attempts to improve cybersecurity is the European Cybersecurity Act (ECA). In the EU, it creates a unified framework for cybersecurity certification that applies to a wide range of ICT (information and communication technology) goods, services, and procedures (Kohler, 2020). The main goal of this framework, as noted by (Kohler, 2020), is to lessen the dispersion of cybersecurity certification programs that are common throughout the European Union. This guarantees a uniform degree of cybersecurity throughout

the European Union, which is essential in a period of growing digital interdependence and transnational data flows.

The European Union Agency for Cybersecurity (ENISA) is also given more authority by the Act. It makes ENISA a central body in the EU's cybersecurity certification framework and greatly expands its responsibilities. According to (Mitrakas, 2018), ENISA's enlarged role entails working with both domestic and foreign parties, offering advice on cybersecurity tactics, and advocating for a uniform strategy for cyber resilience throughout the EU.

2.2.2 European Cybersecurity Act in Standards Development

The European Cybersecurity Act identifies standardization as a fundamental strategy in strengthening cybersecurity across the EU (Kohler, 2020). This strategy is rooted in the understanding that diverse and conflicting cybersecurity protocols can weaken the overall digital defense infrastructure. By advocating for a unified set of security protocols and certifications, the ECA aims to establish a common cybersecurity baseline that is both robust and adaptable. This standardization is not just about defending against current threats but also about creating a framework resilient enough to handle future cyber challenges (Hernández-Ramos, 2021).

A unified standardization under the ECA has several advantages, including easier compliance for businesses across EU countries, lower cost and complexity, and a stronger overall cybersecurity posture. This builds trust in digital products and services, knowing they adhere to high security standards (Garnier, 2018).

The European Committee for Standardization (ECEN), the European Committee for Electrotechnical Standardization (CENELEC), and the European Telecommunications Standards Institute (ETSI) are just a few of the top standardization organizations that the ECA collaborates with to help standardize cybersecurity protocols. These groups are essential collaborators in converting the goals of the ECA into workable, legally binding standards since they offer a multitude of standard-setting knowledge and experience (Smaxwil, 2011).

ENISA facilitates continuous communication between policymakers, business leaders, and cybersecurity specialists. By having this conversation, standards are produced that are applicable to the present state of cybersecurity, practically sound, and technically sound. According to $(\mathrm{al.}, 2020)$, the cooperation intends to produce standards that are adaptable to growing cybersecurity risks and relevant across many industries and technologies, including IoT and AI.

2.2.3 Impact on Certification of Digital Products

The European Cybersecurity Act introduces a distinct framework for categorizing digital products, which is mandatory for tailoring certification standards effectively. This categorization is based on the nature, usage, and potential risks associated with different types of digital products. The framework likely considers factors such as the sensitivity of data handled, the product's role in critical infrastructure, its user base, and the potential impact of cybersecurity breaches (K. Hovhannisyan, 2021).

Under the ECA, certification standards vary based on the categorization of products. Products aimed at consumers, for example, might need a different kind and degree of certification than those used in important industries like energy, healthcare, or finance. In consumer products, privacy and data security may be given more attention, whereas operational resilience and continuity are probably more important in essential infrastructure.

Products deemed as high risk or highly critical and those that are integral to critical services or national security undergo more strict certification processes. This heightened scrutiny ensures that these products have vigorous cybersecurity measures in place to prevent and withstand potential cyberattacks. The certification process for such products might involve rigorous testing, evaluation, and continuous compliance monitoring (Mitrakas, 2018).

2.3 Cyber Resilience Act

2.3.1 Overview

One of the most significant developments in the European Union's strategy to fortify cyber defenses is the Cyber Resilience Act (CRA). The CRA provides extensive laws aimed at implementing strict cybersecurity measures across a variety of digital products. It was developed in response to the growing reliance on digital technology and the increasing threats associated with the digital sphere. Its central goal is to protect both hardware and software, including all products infused with digital elements, against the plethora of cyber threats and vulnerabilities (Mitrakas, 2018). This act is essential in reinforcing the security and resilience of the EU's digital framework, ensuring a safer cyberspace for all its users. The significance of the CRA lies in its holistic approach. Unlike previous regulations that targeted specific sectors or types of digital products, the CRA contains a broad range of hardware and software, aiming to raise the cybersecurity bar universally. This includes everyday consumer products, industrial components, and critical infrastructure elements, reflecting the interconnected nature of modern digital ecosystems (Ananda, 2022).

In summation, the CRA represents a significant leap forward in the EU's endeavor to build a safer and more resilient digital space. By setting comprehensive cybersecurity standards and promoting the security-by-design approach, the CRA aims to protect not just the digital products but also the users and the broader digital ecosystem they exist. Agreed upon politically on December 1, 2023, it sets comprehensive cybersecurity standards for digital products and its implications across the digital landscape will be decisive in shaping the future of cybersecurity in the EU.

2.3.2 Key Provisions

The Cyber Resilience Act (CRA) introduces a comprehensive regulatory framework, applying to a diverse array of products with digital elements (Hernández-Ramos, 2021). This framework categorizes these products into Class I and Class II, based on their level of cybersecurity risk and the potential impact of associated cybersecurity incidents (al., 2020).

Class I products, though considered to carry a lower risk compared to Class II, are still pivotal in the cybersecurity landscape. The classification hinges on a relative risk assessment, where Class I products are deemed to have a higher risk than unclassified or default category products, but lower than Class II products. Notable examples include identity and access management software, browsers and passwords managers, malicious software detection tools, network management and configuration tools. This category also extends to other critical tools such as products utilizing virtual private networks, among several others (Lam, 2021).

It is essential to recognize that the classification between Class I and Class II can sometimes be ambiguous for certain product categories, such as operating systems, which may appear in both classifications. The European Commission is expected to provide further clarity on these classification nuances in future delegated acts and amendments (Lee, 2021).

Class II products are identified as higher-risk items due to their critical role in cybersecurity vulnerabilities. This category typically encompasses products integral to maintaining the security of more sensitive or critical digital infrastructure. Key examples in this category include operating systems, hypervisors, container runtime systems, public key infrastructure and digital certificate issuers, smartcards, readers, and tokens. Additionally, this category extends to include a range of other vital components integral to industrial and cybersecurity environments (Lam, 2021).

Under the stipulations of the Cyber Resilience Act, the integration of security elements from the beginning of product design and development is mandated, not just encouraged. This approach signifies a fundamental paradigm shift in product conceptualization, with a strong focus on embedding security features as intrinsic components of a product's foundational architecture. Instead of treating security as an add-on feature, the security-by-design principle embedded in the Act necessitates a proactive approach. This entails anticipating potential security threats and integrating countermeasures right from the initial stages of product development. Such a strategy is critical in addressing the dynamic and evolving nature of cyber threats, ensuring that products are resilient by design and capable of adapting to future challenges. This forward-thinking approach, as outlined in the Cyber Resilience Act, marks a significant development in product security strategy within the EU's regulatory framework, emphasizing the necessity of integrating robust security measures from the outset of product development.

Under the Cyber Resilience Act manufacturers, importers, and distributors of connected devices ensure compliance with essential security and vulnerability management requirements, encompassing a wide array of products with digital elements capable of direct or indirect logical or physical data connections. These requirements, as specified in Annex I of the Act, are twofold, encompassing both the security properties of the products and the vulnerability handling protocols to be adhered to by manufacturers (Ananda, 2022).

Before releasing a product onto the market, manufacturers are also required to do a thorough assessment of cyber risk. This evaluation serves as assurance that every possible cyber risk related to a product is found and handled skillfully. The risk management procedure entails assessing the product's security, including any third-party components utilized, to make sure they don't jeopardize the device's overall security. This is crucial, especially for products with extensive digital components, which are increasingly targeted in cyberattacks .

In addition, the CRA dictates effective management of vulnerabilities throughout the product's market lifecycle. This includes regular testing, patch management, responsible disclosure programs, and maintaining clear documentation of the product's security features and vulnerabilities. Manufacturers are required to manage and address vulnerabilities continuously, ensuring that the product remains compliant with the CRA requirements throughout its lifecycle. This ongoing process helps maintaining the integrity and security of products long after they have entered the market (Kohler, 2020).

To comply with the CRA, manufacturers are obligated to align with the pertinent conformity assessment regimes. This process necessitates proving adherence to the critical cybersecurity stipulations enumerated in Annex I of the CRA, which encompasses the implementation of security protocols against unauthorized access, principles of data minimization, and comprehensive vulnerability and patch management. Internal conformity assessments to validate compliance with these criteria, formulate an EU declaration of conformity, and attach a CE marking to the product, are added to the list of the requirements.

Finally, it is imperative that manufacturers report any actively exploited vulnerability or security incident impacting the product to ENISA within 24 hours of discovery. They must also inform users about the incident and any corrective measures that can be taken without undue delay after becoming aware of the incident. This prompt reporting is critical for mitigating the impact of security incidents and vulnerabilities (Ananda, 2022).

2.3.3 Impact on Certification of Digital Products

In summary, the CRA brings about substantial changes in the certification landscape for digital products in the European Union. It establishes stringent requirements, necessitates a security-focused design approach, mandates ongoing vulnerability management, and requires conformity assessment and prompt incident reporting. These measures collectively enhance the cybersecurity standards of digital products, ensuring their resilience against cyber threats. The implementation of these certification schemes is expected to have a substantial impact on European businesses, fostering a more vigorous and secure digital market. By compelling manufacturers and distributors to prioritize cybersecurity from the ground up, the CRA not only elevates the level of trust and safety in digital products but also aligns with the broader EU vision of a secure and resilient digital economy. This landmark regulation is poised to serve as a model for other regions, reinforcing the importance of cyber resilience in an increasingly interconnected global digital landscape.

2.4 NIS2 Directive

2.4.1. Overview

The scope of cybersecurity measures inside the European Union is greatly expanded by the Network and Information Systems (NIS2 Directive), which went into effect in 2023, revised the EU cybersecurity regulations that were first presented in 2016. To stay up with growing digitalization and a changing landscape of cybersecurity threats, it updated the current regulatory framework. The resilience and incident response capabilities of public and private entities, responsible authorities, and the EU as a whole, are further enhanced by extending the reach of the cybersecurity regulations to new industries and organizations. The suggestion put out by Sievers states that the NIS2 Directive broadens its scope by including more businesses in already-existing industries and adding new industries to its jurisdiction. The new categories of "important" and "essential" organizations are used to replace the existing categories of operators of critical services and digital service providers to accomplish this expansion. NIS2 streamlines the process of identifying businesses that must comply with NIS obligations by making size the main criterion (Sievers, 2021).

With the EU internal market becoming more digitally connected and the digital threat landscape changing, NIS2 seeks to strengthen network and information system security, which is a critical component of data protection. This directive recognizes the growing interdependence of member states in the digital sphere and the associated dangers in response to the need for a high common level of security throughout the Union.

All things considered, the NIS2 Directive is a major step forward for the EU in fortifying its cybersecurity framework, resolving the issues brought about by a constantly changing panorama of cyberthreats and adjusting to the contemporary digital world.

2.4.2 Updates and Enhancements in the NIS2 Directive

One of the most significant improvements in NIS2 is the expansion of its scope. The new directive shall cover more industrial sections than the previous one. Some of the extended areas include the internet exchange point, domain name system service, or online marketplace. This extension is critical to recognizing the developing profile of digital services and risks linked to new technology and platforms. This makes the scope of the NIS2 broader, hence including these sectors thus strengthening the structure of security that needs to be secured according to the internal market in the EU.

Furthermore, NIS2 lays down a more prescriptive regime concerning security requirements and reporting incidents by an extended number of entities providing digital services

and online platforms. It points out that the whole digital threat landscape is prone to constant change, and there is need for cybersecurity measures to evolve accordingly to fight these effectively. The result is more transparency and stricter compliance mechanisms that include detailed reporting and higher security standards.

The transition from NIS to NIS2 reflects the EU's proactive stance on cybersecurity, showing a commitment to adapt and respond to the dynamic nature of cyber threats. The broadened scope of the NIS2 Directive not only addresses the immediate need for enhanced protection against cyber-attacks but also anticipates future challenges that could arise with technological advancements.

2.4.3 Implementation Challenges and Strategies

The vast range of entities covered by the NIS2 Directive presents a major implementation difficulty. In contrast to its predecessor, NIS2 covers a wider range of industries, including public sector organizations, small and medium-sized businesses (SMEs), and recently classified "important" and "essential" institutions. A methodology that is universally applicable would be unfeasible due to the distinct operational structures, resources, and cybersecurity maturity levels of each of these companies (Skias, 2022).

Achieving the NIS2 criteria is a highly technical undertaking, particularly for small and medium-sized enterprises and organizations with limited cybersecurity expertise. The wider reach of the Directive necessitates specialist infrastructure and knowledge because it covers new technologies and digital services. Furthermore, resource constraints—both in terms of financial inputs and availability to qualified personnel—are a common problem for smaller firms, making compliance an extremely difficult undertaking.

Organizations must use a diversified implementation strategy to overcome these obstacles. Using this strategy, customized compliance frameworks are created considering the characteristics, size, and risk profile of each firm. These kinds of frameworks ought to be flexible and scalable so as to match the unique requirements and capacities of any entity. To successfully address these issues, public-private collaborations are also essential. Partnerships between the public and commercial sectors enable the exchange of best practices, resources, and expertise, which helps smaller businesses close the resource gap and advance a more coordinated strategy for cybersecurity across various industries.

Organizations can also gain from using well-known cybersecurity frameworks and resources, including the NIST Cybersecurity Framework or ISO/IEC 27001. These frameworks give organized guidance on how to achieve NIS2 compliance and propose best practices for handling cybersecurity risks (Malatji, 2023).

It is imperative to reduce the technological complexity involved in implementing NIS2, particularly for firms that lack cybersecurity expertise. This can be accomplished by enlisting the help of outside experts, such as cybersecurity consultants or service providers, who can offer advice on how to comply with the Directive's specifications. For example, ISO/IEC 27001 is widely used in many nations and can facilitate an organization's seamless transition to NIS2 compliance. With updates to address global cybersecurity threats and enhance digital trust, the third edition of this standard, ISO/IEC 27001:2022, offers a more effective approach for enterprises looking to achieve NIS2 norms (Malatji, 2023).

Finally, for companies operating within the European Union, putting the NIS2 Directive into practice is a crucial but challenging task. By comprehending the many obstacles and implementing calculated actions, organizations can successfully negotiate the route to conformity. As a result, the EU's digital environment is made safer, and their cybersecurity resilience is

increased. In addition to being required for compliance, this proactive and strategic procedure is advantageous for the long-term viability and health of cybersecurity.

2.5 Notable Mentions: Data Act, eIDAS, Chip Act

Apart from the main focus on the NIS2 Directive, the European Cybersecurity Act and the Cyber Resilience Act, it is important to highlight other relevant legislative frameworks, including the Data Act, eIDAS, Chip Act, and Liability Act. All of these acts, play a worth mentioning role to the main subject of this thesis, they do add to our understanding of the regulatory environment that surrounds cybersecurity and digital technology by shedding light on the difficulties associated with developing standards and certifying digital products.

2.5.1 Data Act

The Data Act, effective from January 11, 2024, is a key element of the European Union's data strategy, integral to advancing the Digital Decade's objective of digital transformation. It complements the Data Governance Act of September 2023, together facilitating reliable and secure data access across key sectors. This Act is instrumental in establishing fair rules for accessing and using data within the European data economy. It is notably significant in the era of the Internet of Things (IoT), requiring connected products to be designed in a way that empowers users to access, use, and share the data generated. As a cross-sectoral legislation, it provides principles and guidelines applicable to all sectors without modifying existing data access obligations, with an expectation for future legislation to align with its principles.

The Data Act's impact is multifaceted, enhancing innovation, creating job opportunities, and ensuring legal certainty in data utilization. It aims to mitigate contractual imbalances in data sharing, thus fostering an equitable data economy. The Act enables public sector bodies to access private sector data for public interest, enhancing responses to public emergencies. It also plays a crucial role in the EU cloud market by promoting efficient data interoperability and facilitating switching between data-processing services. In practice, this Act allows users of IoT devices to access data generated, fostering competition in aftermarket services, and potentially lowering market prices. It opens avenues for operational efficiency in industries like manufacturing and agriculture, leveraging IoT and machine-learning technologies. The Data Act, therefore, is not just a regulatory framework but a catalyst for a secure, accessible, and efficient data economy in the EU.

2.5.2 eIDAS Regulation

The eIDAS (Electronic Identification, Authentication, and Trust Services) Regulation, a key element of the digital market in the European Union, creates a thorough framework for electronic transactions. It is essential for improving the security and dependability of online interactions and for establishing a predictable regulatory framework. The eIDAS Regulation permits people and organizations to access online public services in other EU nations using their national electronic identification schemes (eIDs). The ability to operate across borders ensures that trust services have the same legal standing as their more conventional, paper-based counterparts, so promoting an internal market for trust services throughout Europe. The principal objective of the regulation is to foster trust in digital interactions by promoting their organic utilization by both citizens and companies.

An open consultation was held as part of the European Commission's evaluation of the eIDAS legislative framework to get input on the evolution and adoption of eID and trust services in Europe. This review took into consideration the experiences of many stakeholders, evaluating how well the framework performed in achieving its goals and adjusting to changes in the market,

technology, and law. The eIDAS rule, which provides solutions for a range of online operations like tax filing, student mobility, bank account creation, and business setup in another member state, has greatly benefited European enterprises, residents, and government services. Its deployment will result in increased online convenience and security, which is essential for safe cross-border transactions and the expansion of the EU's digital single market.

2.5.3 Chip Act

The European Chips Act, adopted by the European Union on September 21, 2023 is an important step toward securing Europe's proper standing in the competitive and rapidly changing market for chips. The regulation includes European involvement in digital and environmental revolutions, with activity levels targeting critical concerns within the semiconductor supply chain. What is underlined by the Act is the importance of semiconductors or "chips" in several industries, among which computer processing, the automobile industry, telecommunications, and a lot more. All these play an essential role in contemporary economies and daily life, laying the essential element of which the continuous digital revolution must be based upon. If one thing has become evident with the latest global chip shortage, which has led to severe product scarcity and upset supply networks, it is that the European Chips Act is long overdue and very much necessary. The proposal also contributes to strengthening the semiconductor capabilities of the EU. Other parts of the initiative include, among others, a recommendation to Member States for supply chain disruptions, changes in the KDT Joint Undertaking Council Regulation, and a comprehensive communication on the Semiconductor Strategy.

By guaranteeing supply chain resilience and minimizing reliance on outside sources, the European Chips Act aims to strengthen the semiconductor ecosystem within the European Union. With a focus on five strategic objectives—improving research and technological leadership, expanding Europe's capacity for innovation in chip design, manufacturing, and packaging, increasing production by 2030, addressing the skills gap and luring in new talent, and building a thorough understanding of global semiconductor supply chains—it aims to double Europe's share of the global semiconductor market to 20% by 2030. Three main action pillars support these objectives. The "Chips for Europe Initiative" fosters innovation and large-scale capacity building in technology, advancing the advancement of quantum and next-generation semiconductor technologies. A framework to ensure the security of supply and resilience of the EU's semiconductor sector aims to attract investments and enhance manufacturing capabilities. Finally, the European Semiconductor Board, composed of Member State representatives and led by the Commission, serves as a coordination mechanism for monitoring the semiconductor value chain and responding to crises with emergency measures. This governance structure, overseen by the European Semiconductor Board, continues the work initiated by the European Semiconductor Expert Group and aligns with the Commission's recommendations for addressing semiconductor shortages and monitoring the semiconductor ecosystem.

3. ISO Standards

3.1 Relevance and Introduction of the Standards

These selected standards offer a comprehensive approach to evaluation, certification, and management of the lifecycle security of cybersecurity risks in the context of a digital product or service.

ISO/IEC 15408-1, defining a general concepts and principles of IT security evaluation and presents a general model of evaluation ISO/IEC 15408-2, referring to the security functional components and ISO/IEC 15408-3, producing a catalog of the security assurance components. These parts of ISO/IEC 15408, known as the Common Criteria for Information Technology

Security Evaluation, detail the framework of IT security evaluation for products and systems. This will include the development and evaluation of security specifications and protection profiles such that there is some sort of basis for mutual recognition of evaluation results between different countries. This standard is important in the sense that it ensures the digital products meet predetermined internationally recognized security criteria, hence their reliability and market acceptance is enhanced (Aizuddin, 2001).

ISO/IEC 18045 is a companion standard and provides the methodology to evaluate target IT systems according to ISO/IEC 15408. This standard specifies the most minor activity to be done by an evaluator to carry out an ISO/IEC 15408 series of evaluations, making use of the criteria and evaluation evidence as defined in the ISO/IEC 15408 series. It ensures equal and strict treatment in evaluating IT security; therefore, it plays a vital role in the certification procedure of digital products that complement the ISO/IEC 15408 (Chen).

Another essential standard in the field of information systems is the ISO/IEC 27001:2022. It focuses on the objectives and requirements concerning an organization to establish, implement, and maintain an ISMS and, finally, improve the ISMS. This standard provides for a structured and systematic approach to the management of sensitive company information to ensure its secure preservation. These include the risk requirements for the assessment and treatment of information security risks according to the needs of an organization (Malatji, 2023).

3.2 ISO/IEC 15408 Series – Common Criteria

3.2.1 Overview

The ISO/IEC 15408 series, known as the Common Criteria (CC) for Information Technology Security Evaluation, is a critical framework in IT security. It originates from the 1990s, which period marks the first earnest attempt at international cooperation aimed at standardizing IT security evaluation by integrating the current national standards in a single frame. The standard evolved from previous security standards, such as the European ITSEC and North American TCSEC, and now represents the outcome of a series of efforts to develop criteria for the evaluation of IT Security, which is broadly helpful within the international community (Aizuddin, 2001).

It acts not only as an index for the user to compare and judge the security characteristics of different IT products but also gives manufacturers a credible standard for assuring that their system meets some security requirements. The CC is, further, a significant reference guide for developing and procuring IT products and systems with robust security functions. It, therefore, gives users the confidence that the IT products or systems they entrust to them meet an evaluated and recognized security standard.

The ISO/IEC 15408 series is flexible and can fit a wide range of products in IT systems to be used in security evaluations according to organizational needs. It states the levels of different evaluation assurances, hence allowing for security evaluation tailored according to needs (Chen).

3.2.2 Key Words & Definitions

Protection Profile (PP)

An implementation-independent statement of security needs for a Target of Evaluation (TOE) type. It describes a set of requirements to counter specific threats within a defined environment. While it may not always present the optimal solution, it aims for consistency, correctness, and completeness by avoiding contradictions and specifying all relevant information needed to address the problem it targets (ISO/IEC 15408-1:2022). As Ariffuddin Aizuddin says, a

Protection Profile is designed to answer the question: “What do I need in a security solution?” (Aizuddin, 2001).

Security Target (ST)

An implementation-dependent statement of security requirements for a target of evaluation based on a security problem definition (ISO/IEC 15408-1:2022). It describes a specific TOE, the conformance claims applicable to the evaluation of the TOE, the security problem to be addressed, the security objectives for the TOE and its operational environment, the security requirements applicable to solving the stated security problem, and additional material necessary for evaluation. STs are generally based upon PPs or PP-Configurations and are typically produced by a developer. As Ariffuddin Aizuddin says, a Security target is designed to answer the question: “What do you provide in a security solution?” (Aizuddin, 2001).

Target of Evaluation (TOE)

A set of software, firmware, and/or hardware, possibly accompanied by guidance, which is the subject of an evaluation (ISO/IEC 15408-1:2022). The Target of Evaluation (TOE) refers to an IT product or system undergoing evaluation, with its security attributes specifically detailed in a Security Target or more broadly in a Protection Profile. Central to the Common Criteria approach is the concept that a product or system should be assessed against a distinct set of criteria outlined in the ST. This evaluation involves thorough analysis and testing conducted. Essentially, the TOE - representing the product - encompasses both the IT product or system and its related documentation for administrators and users, all of which are the focus of the evaluation process (Aizuddin, 2001).

Evaluation Assurance Level (EAL)

A well-formed package of security assurance requirements representing a point on the pre-defined assurance scale (ISO/IEC 15408-1:2022). The Evaluation Assurance Level (EAL) represents the numerical rating that indicates the depth and rigor of an evaluation. Each EAL relates to a set of security assurance requirements (SARs) that span the whole development of a product at a specified level of strictness. Common Criteria defines seven levels, with EAL 1 being the most basic and thus the cheapest to implement and evaluate, and EAL 7 being the most demanding and expensive. Typically, an author of a ST or PP may choose a bundle of assurance requirements, possibly supplementing them with higher-level requirements in specific domains. Higher EALs do not necessarily suggest better results or higher security, they just mean that the asserted security assurance of the TOE has been more thoroughly verified.

Security Assurance Requirement (SAR)

Security requirement that refers to the conditions and processes for the development and delivery of the target of evaluation (TOE), and the actions required of evaluators with respect to evidence produced from these conditions and processes (ISO/IEC 15408-1:2022). These requirements describe the procedures implemented during product development and review to ensure compliance with the claimed security functionality. For example, an evaluation may require that all source code be stored in a change management system or that comprehensive functional testing be carried out. The Common Criteria provides a list of these, and the standards may differ from one evaluation to another. The ST and PP document the requirements for certain targets or product kinds.

Security Functional Requirement (SFR)

Security requirement, which contributes to fulfil the target of evaluation (TOE) security problem definition as defined in a specific security target (ST) or in a protection profile (PP) (ISO/IEC 15408-1:2022). These requirements identify the distinct security functions that a product may deliver. The Common Criteria provide a standardized catalogue of such functions. A SFR, for example, may specify how a user in a specific role can be authenticated. Even if two targets are similar products, the list of SFRs may differ across evaluations. While Common Criteria does not require certain SFRs to be included in a ST, it does indicate dependencies where one function relies on another.

3.2.3 Audience

The interested groups for the security properties of TOEs which are demonstrated by the (ISO/IEC 15408-1:2022) are mainly five. All the ISO/IEC 15408 series is constructed to assist these groups which consist of consumers (risk owners), developers, technical working groups, evaluators, and others.

The ISO/IEC 15408 series is designed to guarantee that assessment meets the demands of risk owners, which is the primary goal and justification for the evaluation process. Risk owners can utilize evaluation results to determine whether a TOE meets their security requirements. These security requirements are often defined through a combination of risk analysis and policy direction. Risk owners can also utilize the evaluation results to compare various TOEs. The ISO/IEC 15408 series provides risk owners, particularly those in consumer groups and communities of interest, with an implementation-independent framework known as the PP, which allows them to articulate their security requirements unambiguously.

The ISO/IEC 15408 series is intended to help IT product developers prepare for and evaluate their TOEs, as well as establish the security standards that such TOEs must meet. These requirements are contained in an implementation-dependent construct known as the Security Target (ST). This ST may comply to one or more PPs to demonstrate that the TOE meets the security needs of consumers as outlined in those PPs. The ISO/IEC 15408 series can then be used to define the responsibilities and actions required to provide the appropriate evidence to support the TOE's evaluation against these standards. It also specifies the content and presentation of the evidence.

The ISO/IEC 15408 series is designed to help technical working groups prepare and build Protection Profiles (PPs), PP Modules, PP Configurations, packages, and accompanying documents or guidelines. Technical working groups can be made up of stakeholders such as customers (risk owners), developers, evaluators, and academics.

The ISO/IEC 15408 series offers criteria that evaluators can use to determine whether TOEs, STs, PPs, and PP-Configurations meet their security requirements. It outlines the overall set of actions that the evaluator must take out. The ISO/IEC 15408 series does not describe the methods to be used when carrying out those actions. The standard's general model, which applies to multi-assurance evaluations, requires the evaluator to analyze the TOE secure functionality to assure the TOE's security.

While the ISO/IEC 15408 series is intended to specify and evaluate the IT security properties of TOEs, it can also be used as reference material by any party interested in or responsible for IT security. The knowledge of this standard can also benefit the following groups like system custodians and system security officers are responsible for defining and meeting the organizational IT security policies and regulations. Auditors, both internal and external, responsible for reviewing the adequacy of the security of an IT solution. Security architects and designers who are responsible for specifying the security features of IT products and accreditors who are in charge of accepting an IT solution for use inside a certain environment.

3.2.4 ISO/IEC 15408-1 Introduction and general model

The ISO/IEC 15408-1:2022 standard, part of the ISO/IEC 15408 series, provides a comprehensive framework for IT security evaluation, stressing the alignment of security evaluations with the needs identified through risk analysis and policy guidance. This standard emphasizes the necessity of understanding security requirements through precise asset identification and security controls, which include both software and hardware components. It emphasizes the importance of successfully communicating security requirements in order to suit the specific needs of consumers or risk owners, while also reflecting the changing environment of cybersecurity threats and the need for adaptive security approaches.

The specification of security requirements is a critical component of this framework, which includes a detailed methodology for defining the security problem, identifying risks, outlining organizational security rules, and establishing security objectives. This foundation enables a full understanding of security requirements and the development of appropriate responses.

The standard also describes the process of defining security requirements, including identifying risks, detailing organizational security policies, formulating assumptions, and developing security objectives for the Target of Evaluation and its operational environment. It uses assurance procedures such as Evaluation Assurance Levels to build trust in a product's security features.

Furthermore, the standard emphasizes the creation of Protection Profiles and Security Targets, which are critical for assuring IT product security. PPs define standardized security requirements for various IT product types, whereas STs outline the security features of unique products. The evaluation process is an important component of the framework because it rigorously assesses whether the security aims and profiles are satisfied and ensures that IT products comply with stated security criteria.

3.2.5 ISO/IEC 15408-2 Security functional components

ISO/IEC 15408-2, a major component of the Common Criteria for Information Technology Security Evaluation, has a significant impact on the landscape of information security. It defines the security functional components that IT goods or systems must have to provide comprehensive protection against a wide range of digital threats. This section of the standard gives thorough guidance on the security features required to protect IT systems, making it a significant resource for cybersecurity developers, assessors, and researchers.

The standard is methodically structured, with security functional components organized into a clear hierarchy of classes, families, and individual components. Each class comprises a large area of security, such as Cryptographic Support or User Data Protection, and covers a range of features required for effective IT security. Within these classes, there are families, which group together components that address similar security objectives, albeit at various implementation levels or methodologies.

Individual components within each family are described in great detail. These components define the specific criteria or capabilities that an IT product should have. For example, in the cryptographic support class, a component may specify the requirements for key generation procedures or the encryption methods to be used. This detailed approach to define security functionality promotes a complete grasp of what constitutes a secure IT system and enables exact evaluation against these criteria.

In the academic world, ISO/IEC 15408-2 is more than just a series of instructions; it is a comprehensive framework for improving knowledge of IT security components. It provides an

organized approach to analyzing and researching various security processes, making it a valuable tool for cybersecurity experts. The standard's extensive definition of security functionalities also serves as a framework for comparative analysis, allowing researchers to evaluate how different IT systems meet these security requirements.

Furthermore, ISO/IEC 15408-2 helps guide the development of innovative security solutions. For individuals working in IT security and system design research, the standard gives a clear framework for incorporating security elements into new products, guaranteeing that these innovations comply with internationally accepted security criteria. The standard's modular form simplifies the complicated terrain of IT security, making it easier to learn and debate. The standard is critical for developing policies that impose basic security criteria in IT systems. Understanding these precise functional criteria in accordance with international standards is critical for researchers and policymakers in IT policy and regulation to establish effective and enforceable cybersecurity policies.

3.2.6 ISO/IEC 15408-3 Security assurance components

ISO/IEC 15408-3:2022, another core component of the Common Criteria for information technology security evaluation, has a considerable impact on the information security landscape. This part focuses on the assurance components required to evaluate and certify the security of IT products. It builds upon the structure established in ISO/IEC 15408-1 and 15408-2, which address the general model and security functional components, respectively, by introducing a systematic approach to security assurance.

The standard's assurance paradigm is based on the premise that security risks and organizational security policies must be properly stated, and suggested security controls must be demonstrably adequate. It emphasizes the importance of preventing, minimizing, and monitoring vulnerabilities in IT products. The assurance components listed in this standard serve as a baseline for developing a clear and structured method to assessing the security assurance of IT solutions.

ISO/IEC 15408-3 is divided into three important sections, each covering a different area of security assurance. The assurance class structure, for example, defines a taxonomy for categorizing security assurance requirements (SARs). These classes are further separated into families and components, with each including special assurance needs. For example, the Development (ADV) class addresses components of the TOE's design, architecture, and development, ensuring that the product is created safely from the ground up.

The standard also specifies criteria for assessing Protection Profiles (PPs), Security Targets (STs), and their configurations. This ensures that the security assurances made regarding IT devices are both theoretically sound and practicable in real-world circumstances. For example, evaluating a PP entails thoroughly examining its introduction, compliance claims, security problem statement, and security objectives. This rigorous examination ensures that the PP appropriately matches the security requirements and expectations for a given type of TOE.

More specifically, ISO/IEC 15408-3 specifies assurance components that are critical for IT product creators, evaluators, and users. Developers utilize these components to help them design and construct secure products. Evaluators rely on them to rigorously analyze the security characteristics of information technology products. Meanwhile, consumers can use these components as a reference to determine the level of security provided by various IT solutions.

3.3 ISO/IEC 18045 - Methodology for IT security evaluation

3.3.1 Overview

ISO/IEC 18045:2022 specifies the technique for evaluating the security features of IT products using the criteria provided in the ISO/IEC 15408 series. This standard is critical in ensuring a planned and systematic approach to assessing the security of IT products.

The basis of this standard is its scalability and depth, allowing for a wide range of IT products while retaining a single focus on security integrity. ISO/IEC 18045 ensures that each product is examined with a level of rigor that meets the complexity of today's cybersecurity concerns by encouraging a thorough assessment process. This method assures that the products not only meet recognized security standards, but also have the ability to withstand emerging and unexpected threats.

One of the key features of ISO/IEC 18045 is its emphasis on a thorough review procedure. This process consists of several tasks and sub-activities, each aimed to carefully evaluate distinct aspects of an IT product's security. For example, the standard specifies specific techniques for analyzing the product's security target, development environment, guidance documentation, life-cycle support, and functional and assurance components in accordance with the ISO/IEC 15408 series.

3.3.2 Examination of the Evaluation Methodology

The evaluation process outlined in ISO/IEC 18045 is a detailed procedure that traverses several steps. This starts with the evaluation of the Security Target (ST); here, the ST document containing the product standards is subjected to review for completeness, consistency, and technical integrity. For products claiming conformance to a Protection Profile (PP), such an evaluation should be carried out to determine whether the PP offers an appropriate representation of the required security objectives and standards. Development evaluation later looks at evaluating the development process of the product, including checking the design documents and implementation details to make sure the product meets the specified security standards and best practices.

In addition, the method includes a review of the product's guidance documents in full, such as the user guides and administrator guides, to ensure that these provide a complete set of instructions for safe management and operation. The Life-Cycle Support Evaluation includes examining processes and mechanisms of product support during its whole life cycle, such as Configuration Management and Secure Delivery Protocols. The approach includes functional testing, which is well sought to establish the security functions as specified within the ST, and penetration testing, aimed at identifying potential vulnerabilities.

The procedure concludes with the Evaluation Reporting activity, which records results in an Evaluation Technical Report. The report shall contain details of the product against its security aim and the standard criteria requirements so that a clear and comprehensive appraisal of the product against the claimed security features can be provided. It ensures that the product not only meets the present security standards but is also resilient to the ever-evolving cybersecurity threats, giving users and stakeholders confidence in the security efficacy of the product.

3.4 ISO/IEC 27001:2022

3.4.1 Overview

ISO/IEC 27001 is an information security management standard widely considered one of the most popular and internationally recognized. On October 25, 2022, the third edition of the standard, ISO/IEC 27001:2022, was published to address global cybersecurity challenges and promote digital trust. This standard offers companies a systematic and organized framework for managing and protecting their information assets against security risks and orchestrates the establishment, implementation, maintenance, and continual improvement of an ISMS, which comprises rules and practices governing data control and usage. The certification procedure entails a thorough risk assessment of the organization’s information assets and associated threats. This method helps enterprises prioritize risk reduction and investment by requiring regular evaluations and treatment plans. Regular risk assessments ensure an organization's security approach matches with its business objectives and allows organizations to make educated decisions about security investments and risks (Malatji, 2023).

A crucial component of ISO/IEC 27001 is its Annex A, which provides a detailed catalog of security controls that organizations can apply and support the conformity with the main standard. These flexible controls are designed for the adaptability to diverse organizational needs and are classified into several categories, including access control, cryptography, physical security, and operations security.

Furthermore, ISO/IEC 27001's compatibility with other legislations and regulations, such as the NIS2 Directive, DORA (Digital Operational Resilience Act), and GDPR, is obvious in how these controls enable regulatory compliance. Thus, the organized approach to choosing and implementing suitable security measures, as suggested by Annex A, not only improves businesses' security posture but also guarantees that they satisfy legal and regulatory duties.

3.4.2 Key Updates from ISO/IEC 27001:2013 to ISO/IEC 27001:2022

Progress in the 2022 update to the ISO/IEC 27001 standard represents significant advancement carefully designed to meet the challenges brought about by ever-evolving digital and cybersecurity landscapes. With the introduction of many new security controls, the standard does a better job of covering the nuanced risks of changing technologies and those not adequately considered within the purview of standard coverage, specifically cloud computing. With the exponential uptake of cloud services, there is a need for very strong security measures, and ISO/IEC 27001:2022 now comes in to add to that. It strengthens those controls which will make an organization maintain ironclad security protocols, even with whatever technological platforms are in use. Moreover, the update offers an improvement in the management of information security incidents in depth. It is against this backdrop that the proposed standard provides a platform for the demands for rapid detection, instant reporting, and effective response that will enable organizations to manage security breaches with high operational efficiency and excellent precision.

ISO/IEC 27001:2022 further fine-tunes its framework and brings significant structural and terminological changes that raise the clarity of the standard and its usability by a larger public, from technical staff to top management. Much more apparent orientation has been given with the revised standard regarding integrating management systems into existing organizational processes, and more weight has been given to the establishment of objectives in harmony with the organization's strategic direction. These improvements facilitate the process of implementation and at the same time manage to make ISMS more adapted to the operational and strategic subtleties of today's companies. This makes the standard more of a pragmatic tool at the different layers of an organization, thus improving its security posture and operating efficiently.

This, however, will further come to light with the revision in the area of risk management, thereby calling for a more profound risk assessment as an organization as part of the ISMS strategy. This would typically entail a thorough assessment of all possible risks that could be

affecting the confidentiality, integrity, and availability of the information, followed by the implementation of bespoke measures to ensure that these are mitigated. In addition, the update brings closer alignment with the global regulatory environment, including GDPR and sector-specific regulations required of an organization to demonstrate compliance within diverse regulatory landscapes. This aspect of the standard is critical because it provides structured and auditable ways of documentation and demonstration of efforts about compliance, which is an organization-wide obligation given the stringent requirements for compliance. Such is holistic improvement within ISO/IEC 27001 that it ensures retaining the reigning status as a cornerstone best practice of information security for organizations around the globe, competently supporting them among the defining complexities a digital world presents.

3.4.3 Advancing Digital Product Certification with ISO/IEC 27001:2022

The 2022 revision of ISO/IEC 27001 introduces significant changes developed to strengthen the certification framework for today's digitally based products, like software applications and services, plus IoT devices. This edition features advanced security controls and an extensive risk management framework, critical to ecosystems in high-risk sectors such as Fintech and Health. These are sensitive areas with great exposure to regulation, and therefore, strong measures must be in place to protect data and privacy, with enormous benefit derived from the most stringent methodologies prescribed by ISO/IEC 27001:2022.

The enhancement on security control with respect to ISO/IEC 27001:2022 is crafted specifically for the protection against breaches of the three main characteristics of the data, which are confidential, integrity, and availability. Therefore, in this era of high frequency and impact in the world of data breaches and cyber-attacks, such enhancement is imperative. Organizations abiding by these guidelines hint that there is more to this than just keeping sensitive information; they further develop a basis for trust from users and stakeholders who are expecting the highest levels of security for their data.

Getting certified under this standard is an attestation of organizational commitment to doing robust security practices. This will surely enhance the level of confidence from consumers and regulatory bodies in the certified entity as a reliable and trusted handler of their digital information. This trust is crucial not only about customer satisfaction but also in the considerable reputation of the organization in the market of digital products.

The standard requires continual assessment and improvement in security measures. That process ensures the security practice is not compliant only at the moment of the certification, but it also follows the development according to new threats and technologies. This dynamic compliance, in return, ensures that in the face of new threats and vulnerabilities, their digital products and services can be more resilient.

Adoption of the ISO/IEC 27001:2022 standard, therefore, operationalizes compliance with international regulations, including the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA). It provides a systematic approach to risk management related to information security, covering operations on an international level and transfer of data.

Finally, the kind of certification to conform to ISO/IEC 27001:2022 brings any organization a competitive advantage. This signals to potential clients and partners of a company or an entity in which such advanced security measures are highly valued and have been put in place. This is, therefore, very critical in those markets where consumers and businesses are increasingly ranking digitized security as one of their highest items in awareness and preference lists. ISO/IEC 27001:2022 introduces significant strategic changes, enhances the information security management framework, and requires it to be mandatory for the adherence of all organizations

in or around the development and deployment of digital products. These advances would not only fortify the security of such products but also set the stage for organizational efforts of broader scope that would be aimed at a more robust security posture against growing and evolving cyber threats.

4. Case Study of Auditing an ICT Company against ISO/IEC 27001:2022

This chapter considers an illustrative case of "Tech Innovators Inc.," a key provider of AI-driven and ICT digital products. A case study will illustrate the conduction of an audit in line with ISO/IEC 27001:2022 and the impact such an audit could have on the company's digital products and general cyber posture. The focus will be on the activities preceding the audit, the process followed during the audit, the activities that follow the audit, and finally, the impact of the audit-certification on the digital products. It will provide an overview of the practical application of the ISO/IEC 27001:2022 standard, along with the benefits and challenges of the certification process.

4.1 Introduction of the Company

4.1.1 Company Background

The beginning of Tech Innovators Inc. was in 2010 with a visionary group of engineers and technologists with a mission and vision for changing innovative digital provisioning with creative, safe, and scalable products through cutting-edge artificial intelligence and information communication technology solutions leading the globe in the market for ensuring improvement to the level of businesses' efficiency and the elevation of quality life. Over the decade, Tech Innovators Inc. has become one of the titans in the tech arena, known for excellence, innovation, and cybersecurity.

Tech Innovators Inc. was realized across most parts of Europe, focusing on IT customers. The customer base is very diversified, cutting across software developers, companies that offer IT services, and technology startups. What is more important is the fact that the subject company has developed a partnership with IT companies scattered all over Europe, which have the best cybersecurity that one can find. More than 200 European businesses put their trust in the products and services of this company, adding further weight to its credibility as a reliable and innovative technical partner.

4.1.2 Company’s Products

Tech Innovators Inc. specializes in developing a wide array of AI-driven analytics platforms and the provision of cloud services. The company's product portfolio includes that is in the scope of the ISO/IEC 27001:2022 audit will be the following.

AI-Powered Analytics Platforms

The organization provides AI-powered analytics platforms that process and analyze large volumes of data. Modern algorithms guide the offered platforms to gauge conclusions and predictive analytics in identifying trends, forecasting outcomes, and making effective decisions.

Overall, these platforms can process data in real-time, allowing companies to push decisions right at the point of action, have data visualization tools, which help to make even the most complex data sets visually understandable and use machine learning models that adapt to changing data patterns.

Cloud Computer Services

Tech Innovators Inc. offers highly scalable cloud computing services that provide secure and flexible solutions in information storage, computing power, and application hosting. These solutions also offer reliable, cost-effective, and adaptable cloud environments that emanate from

initiatives in digital transformation. It provides features such as preconfigured virtual machines that offer ready, customizable, and flexible computing resources, container services that ease the development, deployment, and management of applications in lightweight and portable containers, and ensured secure cloud storage solutions propagating data integrity and access from anywhere.

4.2 Description of the ISMS

This chapter discusses the extensive preparation that Tech Innovators Inc. went through regarding the ISO/IEC 27001:2022 audit. These preparations are justified by the company's philosophy of delivery in securing innovative and scalable AI-driven platforms and cloud services. The rest of this section highlights the detailed steps carried out to prepare for the audit requirements, with emphasis placed on the areas to be assessed.

4.2.1 Framework

Tech Innovators Inc. conducts all its activities to serve the needs and expectations of its customers in the most efficient and secure manner. To ensure the best possible satisfaction and protection of its customers' data, the company's management ensures the optimal operational condition of its facilities and the high quality of the results of the projects it undertakes, with special care for information security. The company's management believes that continuous improvement of the security level of the information managed by the company is required, so that the quality of business activities remains competitive and the implementation of a security management system with elements that allow for self-assessment and improvement is a strategic choice to achieve this goal.

4.2.2 Scope

The scope of the Information Security Management System at Tech Innovators Inc. covers all critical areas that are related to the core activity of the company. For the purposes of the ISO/IEC 27001:2022 the scope is described as follows:

IT support, cloud services, design, and production of AI-based analytics platforms

This will ensure that there is systematic protection for all information assets, processes, and systems in this area, with a wide coverage of all possible security threats. The ISMS in place provides coverage for the full lifecycle of these services and products, from initial design to deployment, support, and ongoing management. By clearly defining the scope to include these key operational areas, Tech Innovators Inc. ensures that the ISMS is both comprehensive and aligned with its business objectives, particularly in safeguarding the confidentiality, integrity, and availability of its digital products and services. This will also establish the boundary within which the ISMS operates, and it will be focused on related departments, physical locations, and IT infrastructure.

4.2.3 Policies and Objectives

Tech Innovators Inc. conducts each of its activities in such a way, to serve the needs and expectations of its customers in the most efficient and secure manner and considers the applicable standards, legislation, regulations, as well as their application guidelines in all its activities and undertakes to comply with them. The company's management believes that continuous improvement of the level of information security that the company manages is necessary, so that the quality of business activities remains consistently competitive. The implementation of a security management system with elements that allow for self-assessment and improvement is a strategic choice aimed at achieving this goal.

The Security Policy is a cornerstone of the company's Information Security Management System. Therefore, frequent changes to it are not anticipated. However, because the environment changes rapidly, the Policy is being reviewed periodically to ensure its continued suitability and is modified accordingly, if necessary, at least once a year.

The management implements all the company's policies across the entire organization. The implementation and effectiveness of these policies are also monitored. Staff awareness is regularly assessed, and security incidents are promptly identified, and corresponding corrective and preventive actions are taken. Some of these policies and documentation are: Backup Policy, Compliance with applicable standards and regulations, Information Exchange Policy, Partner and Service Provider Policy, IT Asset Register, Physical Access Security Procedures, Risk Assessment and Risk Treatment Methodologies and Plans, Clean Desk and Clear Screen Policy, Password Policy, Use of Removable Media, Media Disposal, Software Configuration and Change Management Procedures, Business Continuity Plan, Teleworking Policy, Technical Vulnerability Management, Information Classification & Labeling.

The main objectives of implementing an Information Security Management Systems for tech Innovators Inc., consist of improving Risk Management related to information security, preventing situations that could potentially have legal implications for the company, minimizing the recurrence of information security incidents, enhancing incident management, increasing staff awareness, and providing a common framework for information security. All these objectives ultimately aim to increase confidence that the system will lead to the secure and confidential management of information and customer data.

4.2.4 Risk Assessment and Management

For Tech innovators Inc., Information Security is defined as the protection of Confidentiality, Integrity, and Availability of Information. Risk is defined as "the occurrence of an undesirable situation" and has two main characteristics based on which it is assessed:

The likelihood of a threat occurring and the impact it would have if it does occur.

The basic analysis for the risk assessment is conducted through questionnaires completed by the responsible parties in each involved area. Initially, they are asked to assess the threats probability as High (3), Medium (2) and Low (1). High with a score of 3 means that the specific threat has high motivation and the necessary capability. Related incidents are frequent (1-2/month or more). Medium with a score of 2 means that the threat has relative motivation and capability, and the number of previous similar incidents was small. Low with a score of 1 means that the threat has no motivation or capability, and that rare incidents have been recorded.

Next, they are asked to identify the impact on the confidentiality, availability, or integrity of information. The impact is evaluated as High (3), Medium (2) and Low (1). High with a score of 3 means that the impact could lead to very high-value damage or destruction of resources or assets or significantly violate, harm, or impede the mission, reputation, or interests of the company or lead to severe injury or death. Medium with a score of 2 means that the impact could lead to costly damage or destruction of resources or assets, or violate, harm, or impede the mission, reputation, or interests of the company or lead to injury. Low with a score of 1 means that the impact could lead to damage or destruction of resources or assets or affect the mission, reputation, or interests of the company.

Finally, the risk is calculated as the product of the Probability Score X Impact Score. Risks with a score of 1-4 are considered acceptable, while those with a score above 4 are considered unacceptable.

For each risk, a risk owner is assigned. Unacceptable risks are communicated to Management, which decides whether to manage the risk or accept it. Risks that are decided to be managed are assigned to the Information Security Management Officer for identifying the necessary controls to mitigate or eliminate them.

The actions decided upon are recorded in the Risk Treatment Plan, and if required, are monitored through the Corrective Actions process. Once the actions are implemented, the risk assessment is repeated to identify the residual risk. If the residual risk is rated 1-4, it is considered acceptable. If the score remains above 4, the process is repeated.

The risk is assessed to be addressed immediately. In this case, immediate actions that can be implemented are selected in collaboration with the Information Security Management Officer, the residual risk after their implementation is assessed, and the proposed actions are submitted to Management for immediate implementation. If more than one action is possible, Management, in collaboration with the Information Security Management Officer, selects the actions and informs the responsible party for implementation. The immediate actions implemented, and the residual risk are recorded in the Risk Assessment document. If additional actions need to be scheduled, they are recorded in the Risk Treatment Plan.

Actions that do not need to be implemented immediately or require significant time for implementation are placed on a management list. Depending on the calculated risk score, the time required for their implementation, and the necessary resource costs, the planned actions are prioritized. Each action is clearly assigned a planned completion date, a responsible implementer, and a responsible verifier. Upon completion of the actions, the Information Security Management Officer calculates the residual risk and records it in the Risk Assessment. The above are documented in the Risk Treatment Plan, which is an integral part of the Risk Assessment.

The risk coming from the risk assessment procedure, or the residual risk is accepted by Management and introduced as an item for discussion during the next Management Review.

4.2.5 Implementation of Controls

Tech Innovators Inc. has produced a thorough Statement of Applicability, which describes the required controls aimed at mitigating identified risks within its full scope.

This began with the application of the controls deemed appropriate from Annex A of ISO/IEC 27001:2022. These controls are that which proves to be the most effective against risks identified in the previous risk assessment. Prioritized technical controls such as encryption, access control mechanisms, and intrusion detection systems ensure the protection of sensitive data processed by AI algorithms and cloud services. Moreover, implementing security policies, procedures, and training programs were devised for administrative controls to really inculcate a strong security culture in the organization.

Implementing these was done by making these controls part and parcel of the information systems and workflows of the company. Incorporate technical controls such as data encryption and MFA into the company's IT infrastructure with respect to protecting the data at rest and in motion. For instance, MFA was introduced to all systems of login as a further step to ensure that, in the event passwords fall into the wrong hands, no unauthorized access would be allowed. The careful planning of rollout assured that business operations were not disturbed and that new controls really reinforced overall security but did not cause major inconvenience for users.

In parallel with the above technical implementation, Tech Innovators Inc. also created and disseminated formal security policies and procedures. These documents established a clear direction of how information security management would be executed, with specific steps to be in line with ISO/IEC 27001:2022.

Along similar lines, the company engaged in extensive training and awareness programs so that all employees knew their respective roles and responsibilities regarding information security. The programs were established to familiarize staff with the importance of information security, relevant controls, and work practice. Regular training sessions covered all fronts, from

the recognition and reaction to suspected security incidents, the correct usage of security tools and protocols, to the maintenance of compliance with company policies.

Continuous monitoring and regular reviews were established as critical components of the control implementation phase. Tech Innovators Inc. has applied advanced monitoring tools to monitor security incidents in real time and assess the effectiveness of applied controls. The real-time alerts and comprehensive reports concerning security events, generated by these tools, have assisted the company in detecting potential threats and responding rapidly to them. Internal audits and management reviews were scheduled to carry out a review into the implementation and effectiveness of the controls, so that potential weaknesses or areas for improvement could appropriately be acted on.

4.2.4 Additional Requirements

Tech Innovators Inc. documents in detail all areas of the implementation of ISMS to show conformance with ISO/IEC 27001:2022. Such documentation forms the main basis for the audit, with evidence such as full records in relation to corporate needs and general business and statutory requirements. The security policy describes the commitment of top management to information security, the scope of the ISMS, and general goals related to keeping information's confidentiality, integrity, and availability. Detailed reports have been made of the risks assessed, the impact and likelihood of assessed risks, and the mitigation strategies for those risks. The reports provide a holistic view of the company's risk landscape and illustrate a systematic approach toward the identification and mitigation of potential threats.

Records of security incidents, along with response and resolution procedures taken, were taken meticulously. Such records could be used to show the effectiveness of the incident management process and evidence as to how the company responded to and resolved security incidents.

There are also procedures on reporting of incidents, investigation, and measures for corrections. Internal audit reports which were conducted through a checklist, were produced to establish whether the ISMS conformed to ISO/IEC 27001:2022 requirements. The non-conformities were identified from such reports as a way of continuous improvement. Through the recording of findings of the audit and corrective actions, as well follow-up actions, there was the achievement of the effectiveness and conformity of the ISMS to the standard.

Other supporting documents include SWOT analysis, metrics and KPIs used to measure the effectiveness of the ISMS, evaluation of critical suppliers regarding information security along with SLAs and NDAs, Management Review records, Awareness and Training records, documents related to compliance with relevant legal and regulatory requirements, Backup and Recovery Logs and Communications and Awareness Campaigns.

4.3 The Audit Process

The idea of an external audit by a certification body is that it constitutes independent verification with the goal of the organization's compliance with specific standards, in this case, ISO/IEC 27001:2022. Unlike internal audits, which are conducted by the organization's staff to achieve conformity and improvement objectives, an external audit gives an unbiased assessment from a third-party view. In such objectivity, therefore, lies the credibility of the results of the audit, where the feedback will also be impartial.

An external audit in the context of Tech Innovators Inc. should aim to confirm the efficiency of the Information Security Management System and its compliance with cybersecurity

standards. The following are the activities and procedures that an external audit would encompass, representing the phases it would have to pass through to ensure a thorough review of the organization's security posture.

4.3.1 Pre-Audit Activities

Pre-audit stage is the process in which Tech Innovators Inc. engages the external auditor. During this phase, the two parties engage in detailed planning to determine the amount of time to be used and when. This communication is the most essential as it provides a structure for the whole auditing exercise. The firm communicates with Tech Innovators Inc. to arrive at a workable time frame by discussing the availability calendars of key personnel and the readiness of the company.

Moreover, the audit team is put together by the certification body considering the complexity of the management systems within Tech Innovators Inc., hence there will be a way to make sure that auditors have the necessary knowledge, skills, and experience specifically for the sector in effective performance of the audits.

It is important, therefore, to confirm the extent of the audit so that relevant areas are not left in isolation. The proposed scope of the audit with regards to systems, processes, and locations being subject to audit is reviewed by the external auditor and confirmed. This way, the audit will be assured to relate to the company's ISMS and the critical areas being underlined through risk assessment. This remains a requirement that both parties are satisfied with the scope so that there are no lapses in the process of evaluation.

Review of prepared documentation is a very important preliminary step. The external auditor goes through all documentation and prepared evidence. The audit will encompass scrutiny of policies, procedures, risk assessment, and implementation of the controls meant to meet the requirements of ISO/IEC 27001:2022. This makes it clear if the ISMS is working well regarding the implementation of controls. The certification body may also insist that Tech Innovators Inc. inform the certification body of any ISMS-related information that the certification body deems unable to be auditable because of its confidentiality and sensitivity. It is the Lead Auditor's decision if, in the light of such information insufficiency, the ISMS can still be properly audited. If it is established during the audit planning and preparation procedures that the ISMS cannot be effectively audited without access to information considered sensitive or confidential, this fact is communicated to the client along with a clear statement that the certification audit cannot continue until appropriate access arrangements are made.

The audit kick-off meeting is a fundamental part of the audit engagement process. It is that first meeting with major interested parties, where the audit process, objectives, and expectations will be discussed. It guarantees that the objectives, timing, and criteria applicable to auditing the ISMS are well understood by all the stakeholders. This will also allow stakeholder concerns or questions about the auditing process to be raised. The audit program shall include the use of network-supported methods to make possible the teleconference, web meetings, interactive web-based communications, or remote electronic access to the documentation or processes of the management systems.

4.3.2 Stage 1 Audit

This was a critical Stage 1 audit for Tech Innovators Inc., with the view to assess its preparedness for the on-site assessment. This was a well-laid-out review covering all the important documentation, considered requisite in the context of the ISMS, for conformance to the norms of ISO/IEC 27001:2022. The auditor wants to understand how the ISMS is designed in relation to the policies and objectives of the company in assessing the state of preparedness for the full audit.

The analysis of the ISMS policy and objectives concerning the general business strategy and ISO requirements was considered at the very detailed level during the first stage of the audit. The ISMS scope was assured as sufficient to cover all related areas of the organization for the provision of AI-based analytics platforms, cybersecurity solutions, IoT systems, cloud computing services, and means of communication, considering both development and design aspects, as well as production ones. At that time, the auditor was assessing the procedures and controls of the ISMS to see whether they be fitted the company's operations, for example, the aspect of access control, encryption protocols, and incident response policies.

The appropriateness of the risk assessment methodology was tested for identification, evaluation, and prioritization of risks. In particular, the auditor examined the way Tech Innovators Inc. identified potential threats, such as cyber-attacks, data breaches, system failures, human errors, and natural calamities. In concrete terms, the risk treatment plan specified concrete actions for reducing the occurrence of identified risks while incorporating the controls of Annex A of ISO/IEC 27001:2022. The auditor focused on whether those controls were in place and whether the strategies for treating the risk were enough. Planning, operating, and controlling the procedures in the information security and privacy processes had to be examined with the applicable ISO standards.

Relevant areas of Tech Innovators Inc. were visited during the site visit. The auditor interviewed employees to assess their understanding and implementation of the ISMS requirements. These interviews provided insights into employee awareness and the practical functioning of the ISMS in daily operations. The performance of key system requirements, including key performance indicators, significant aspects, processes, objectives, and the operation of the management system, was reviewed. The scope of the management system, processes, and sites was verified, along with statutory and regulatory compliance aspects. Documented information was monitored to ensure that internal audits were planned, and management system reviews conducted.

While a few weaknesses have been found, the Stage 1 audit has been able to find numerous strengths. Tech Innovators Inc. has an ISMS policy that is well documented and excellent, but the connection of these policies to organizational objectives was missing, making clear the scope document that was thorough and transparent in setting the limits and boundaries of the ISMS, including all important areas. There were documented policies regarding access control and encryption, and the procedures and controls put in place by the ISMS to support these policies were also sound, but the auditor felt that more detailed implementation guidelines needed to be provided for some of the technical controls.

The risk assessment methodology was thorough, but more frequent updates were recommended to keep pace with the changing threat landscape. The risk treatment plan addressed significant risks, though documenting the rationale for selecting specific controls could be clearer. During the site tour, the auditor noted high employee awareness of the ISMS. Employees understood their roles in maintaining information security, reflecting effective training. The system’s status and understanding of key performance indicators and significant aspects were well-reviewed, with processes and objectives clearly defined. The scope verification confirmed that all relevant areas, including statutory and regulatory aspects, were covered. Internal audit planning and management system reviews were well-documented, showing systematic and thorough approaches to maintaining compliance and continuous improvement.

Tech Innovators Inc. had a well-prepared documentation framework, showing a strong commitment to information security. The detailed records, comprehensive risk assessments, and robust controls provided a solid foundation for the Stage 2 audit. The company’s proactive approach to addressing gaps and improving documentation and processes ensured readiness for the next phase of the certification audit.

4.3.3 Stage 2 Audit

The Stage 2 audit will seek to provide assurance in the management of systems and security programs at Tech Innovators Inc. This is accomplished not only through compliance but also by following its policies, aims, and procedures towards ISO/IEC 27001:2022 requirements. This phase evaluates the effectiveness of controls over deploying, monitoring, measuring, and reviewing service management objectives, plans, and processes.

The auditor undertook various key activities during the on-site assessment, such as interviewing important individuals and observing controls in practice across departments. Evidence collection required logs, incident reports, and monitoring data to demonstrate that the controls were working. The auditor tested these controls thoroughly to validate whether they were operating as designed and addressing the known risks. It was crucial to verify compliance with ISO/IEC 27001:2022, identify any gaps, and document them.

The audit examined several critical areas in Tech Innovators Inc. Firstly, top management's commitment and leadership regarding information security policy and objectives were reviewed, along with their competency in managing risks associated with information security and privacy programs. The documentation supporting the ISMS was investigated, including documented statements of ISMS policy and objectives, the scope of the ISMS, and related procedures and controls. This audit included the risk assessment methodology, a risk assessment report, and verification that policies are adequately designed to ensure appropriate planning, operation, and control of information security and privacy processes. It confirmed that all required records and the Statement of Applicability were being retained.

The audit assessed control objectives according to the risk assessment and risk treatment processes, ensuring they met information continuity requirements. This involved examining the effectiveness of the ISMS, evaluating how well information security controls were working, and performing internal audits on the ISMS along with management reviews. The audit authenticated that the current controls were selected to meet the ISMS policy and objectives, aligned with risk assessment and treatment processes.

A detailed examination was done during the implementation of controls to determine whether they were delivering the stated objectives. The auditor evaluated programs, processes, procedures, documents, internal audits, and reviews of ISMS effectiveness against management decisions. The sufficiency concluded that sets were in place to ensure compliance and traceability, documented by relevant records.

4.4 Impact of the New Controls

4.4.1 Audit Results

Proper execution of ISO/IEC 27001:2022 at Tech Innovators Inc. generally improved their Information Security Management System, which combined the requirements from the business, legal, statutory, regulatory, and contractual perspectives. This audit resulted in numerous findings for improvements in different areas of the company's operation. Top management showed a strong commitment to maintaining and improving the ISMS by regularly reviewing it and ensuring updates to the policies related to the same were well-reasoned for effectiveness and relevance. This proactive stance was important in maintaining pace with the changing threat landscape. Implementation of a full threat intelligence program enabled the organization to monitor and analyze potential threats in real-time for proactive mitigation actions. The employee education and training on how to identify security threats and report them instigated an organizational culture of vigilance, thereby enhancing the security awareness among them. Controls around cloud

service-related information security management had also improved. This included stringent processes for the acquisition, use, management, and exit from cloud services, safe zone encryption, and access controls to mitigate the risks significantly against data breaches and secure the company's cloud operations.

The company was particularly pleased that the audit acknowledged its capable incident response. The process of developing and testing a comprehensive incident response plan has been completed to provide a prompt, consistent response if information security incidents occur. This established clear protocols of communication in giving information to appropriate stakeholders for transparency and organized response processes. The law's requirement on compliance in protecting Personal Identifiable Information (PII) was fully met. To ensure compliance with all laws and regulations on the protection of PII, such measures had been institutionalized. Periodic audits and assessments ensure continuous compliance of data protection laws by institutions, hence safeguarding sensitive information and stakeholder trust. The Configuration Management processes were enhanced, and their procedures made sure that hardware, software, services, and networks worked only with the required security settings. Avoid configuration unauthorized or incorrect changes through continuous monitoring and approval procedures. These processes maintained intact the integrity and reliability of the company's IT infrastructure.

Tech Innovators, Inc. has also initiated a secure erase protocol and created data retention policies to prevent the unnecessary exposure of sensitive information. Data masking techniques minimized the exposure of sensitive data, including personally identifiable information. Proper and full access controls were implemented to prevent unavailability, unauthorized access, modification, or public disclosure of any information. Proper procedures were applied to make sure that not a single piece of information was lost and its confidentiality and integrity could be maintained. Advanced control joins deployed on top of the prevention from data leakage, which can detect and prevent any unauthorized disclosures and extraction of information. In that respect, the company can instantly detect and avert data leakage-related incidents by continuously monitoring the networks, systems, and applications. Steps such as these strengthen further Tech Innovators Inc.'s commitment towards having in place a high standard of information security through the laying down of a proper framework through which it can have a present and future managing framework for security threats while at par with the changing digital times.

4.4.2 Threat Intelligence

Setting up threat intelligence controls took the form of placing a specialized team at Tech Innovators Inc. that would select, collect, and analyze any threats to information security through a structured cyber threat intelligence lifecycle. These phases include setting directions, collection, processing, analysis, dissemination, and feedback. The process started with the setting of goals for the threat intelligence program, followed by understanding the organizational aspects that needed protection and finally the kind of threat intelligence to collect in protecting the assets and monitoring responses to threats. Data was gathered from several sources: internal network metadata, threat data feeds from credible cybersecurity organizations, interviews with stakeholders, and from open-source news sites and blogs. The data was subsequently formatted into a format that the organization could use, and it was then checked for accuracy and reliability by fact-checking and cross-referencing.

The processed data was then analyzed to turn it into actionable intelligence, guiding decisions on security resource investments, investigations into particular threats, actions to block immediate threats, and determination of threat intelligence tools that might be necessary. The results of the analysis and recommendations were communicated to relevant stakeholders in the organization, according to the terms that would suit different teams best. Feedback from these stakeholders was important in fine-tuning and making the threat intelligence program a continuous process—iterative by nature—but also not something that stops once and completely goes away.

The biggest challenge in relation to these tools was their integration with existing systems in such a way that would not be non-intrusive so as not to affect any ongoing operations. It was therefore possible to make threat intelligence an integral part of security protocols within the company seamlessly by phased approach and testing, bringing maximum proactive defense capability against newly emerging threats.

4.4.3 Information security for use of cloud services

In consideration of information security for cloud services, Tech Innovators Inc. had put in place a comprehensive process for the acquisition, utilization, and management of cloud services. Since the company offered cloud security services and used almost all its own products, there were fewer changes it had to implement. However, this control helped the company understand the needs of customers in terms of security. This involved the enforcement of inherent controls that would prevent data leakage, such as strong encryption protocols across all transport layers and secure file shares. Strong authentication—multi-factor authentication—ensured access was granted only to relevant personnel with authorized credentials. The company has also rolled out some of the visibility and threat detection tools to be able to monitor cloud environments in real-time for identifying and mitigating potential security incidents. Tech Innovators Inc. integrated a next-generation WAF to protect applications, mostly modern cloud-native distributed apps. The WAF granularly inspected and controlled traffic to and from the web application servers and updated the rules dynamically in respect of changes to the behavior of the traffic. By bringing the WAF closer to microservices running workloads, Tech Innovators made sure security controls were utilized where they are most required, providing better defense against web-based threats as if applied symmetrically.

Another key part of the cloud security strategy was continuous compliance. Continuous compliance risk management processes should be designed to let the company address regulatory requirements and industry standards. Put differently, it means keeping good hygiene in data storage resources by detecting misconfigured buckets and terminating orphan resources. In doing these, Tech Innovators Inc. reduced their chances of data exposition, making sure that cloud storage resources are managed in a secure way. Some of the enhanced security procedures included encryption of data at rest and in transit through secure communications protocols. This was accompanied by regular audits for adherence to security policies. Security controls were integrated across various security elements and protocols for a uniform mechanism of defense against potential risks to all cloud services. Through this process, Tech Innovators Inc. not only hardened its own security posture but also gained valuable insights into customer security requirements that improved the overall quality and reliability of its cloud services. It delivered a strong cloud security framework, ensuring sensitive data protection, regulatory compliance, and security posture for the company to boldly harness the power of cloud technologies in its operation and to deliver better security solutions to various clients.

4.4.4 ICT readiness for business continuity

The implementation of this control was very beneficial in getting the company well-prepared both for tackling different incidents and ensuring continuous operations. The ICT readiness for business continuity (IRBC) principles on incident prevention, detection, response, recovery, and continual improvement all contributed to the company's resilience and reliability of services. Incident prevention was rigorously applied, hence stringent measures that were put in place to safeguard the ICT services against threats from environmental and hardware failures, operational errors, malicious attacks, natural disasters, and so forth. Advanced monitoring systems and redundancy in infrastructure reduced the occurrence of service disruption to a minimum and ensured high availability of the systems. Incident detection improved considerably as the sophisticated detection tools provided for early identification of issues that turn into incidents. Real-time monitoring and automated alert systems enabled the IT team to act quickly to resolve

problems before service deteriorated, reducing recovery effort. Detailed incident response plans were drawn up to make sure the different types of responses would be appropriate and effective so less important incidents did not grow into big problems.

It involved exhaustive planning and prioritizing the recovery strategies to be adopted that would ensure timely resumption of critical services. Services were ranked in order of priority for recovery by Tech Innovators Inc.: the most critical ones, which included those that would sustain data integrity and not add to the reduction of downtime, were recovered first. Then there were the noncritical services to be recovered later in an organized and effective process. The approach of the company also had continuous improvement imbued within it: lessons learned from previous incidents were documented, analyzed, and reviewed. The company could keep learning in a continuous cycle and constantly work on the refinement of its strategies, improvement of incident management protocols, and preparedness. Dealing with the root causes and executing preventive steps, Tech Innovators Inc. further consolidated its resilience and preparedness for potential disruption that might eventually come to pass. Overall readiness of ICT applications ensured a robust and proactive approach toward counter-threat preparedness in terms of protection of operations, integrity of data, and customer confidence in the company's ability to offer digital products and services that are reliable and secure.

4.4.5 Configuration management

Configuring management controls in Tech Innovators Inc. has significantly changed things about security and functionality of their products. Using NIST SP 800-128 as the guide, Security-Focused Configuration Management of Information Systems, this enterprise ensured that hardware devices, software, services, and networks configurations were established, recorded, executed, monitored, and reviewed with good rigors. This holistic view allowed the integration of security requirements into the configuration management processes quite easily, ensuring that all the components would function as expected with the right security settings and avoiding unauthorized or even wrong changes that undermine the systems.

The rigorous process of configuration identification and recording on the security posture of their systems was developed following the NIST guide. This meant that any update or change was thoroughly subjected to security risk assessments before it was approved, so vulnerabilities couldn't find a way in. In enhancing predictive analytics capabilities, for example, the company has run rigorous tests to establish that new algorithms cannot create backdoors for cyber-attacks. It is through such careful vetting processes that AI-powered analytics platforms and cloud computing services have been secured and made reliable. This corporate commitment to studying the implications of security changes prior to any implementation delivered products that clients could trust for holding their data processing and storage requirements.

This went hand in hand with ensuring that configurations at Tech Innovators Inc. were regularly checked and changed to ensure integrity and reliability of their offerings. Documentation of every change, coupled with continuous compliance checks, reduced the risks of a data breach or disruption of services to near zero. It provided a proactive stance that could detect any unauthorized changes or anomaly early enough, thereby reinforcing an organization's security posture. Tight access controls and robust encryption procedures were therefore put in place to provide a cohesive mechanism of defense across all products. Due to the diligent process taken, it not only secured their AI and cloud solutions but also established trust with their clients by underlining the commitment of Tech Innovators Inc. toward information security best practices and operational excellence.

4.4.6 Information Deletion & Data Masking

Controlling the deletion of information and data masking at Tech Innovators Inc. has been very instrumental in securing sensitive data, especially given the high stakes involved with personal data by their AI-powered analytics platforms and cloud computing services. The company followed the media sanitization guidelines of the NIST Special Publication 800-88 to ensure information deletion from systems, devices, or any other kind of storage media when such data was no longer in use. This process of rendering data unrecognizable and irrecoverable became very important in preventing the unnecessary exposure of sensitive information and meeting legal, statutory, regulatory, or contractual requirements for the deletion of information. By following these rules strictly, Tech Innovators Inc. minimized the possibility of data leakage and unauthorized access to a minimum, thereby preserving the integrity of their products and securing customer trust.

Effective deletion of information is very critical to a firm like Tech Innovators Inc. in general, where sensitive and personal data becomes huge. Making sure that such data is safely deleted reduces the possibility of a data breach; it also helps to avoid legal and fiscal consequences resulting from many regulatory requirements. In this context, during the decommissioning of their servers or replacing the storage devices used by their cloud computing services, this company has followed rigorous sanitization procedures to make sure residual data should not be recoverable. Such an attentive approach to data erasure ensured that the AI-based analytics platforms and cloud services worked under a safe regime of protecting user data, giving meaning and reinforcement to this company's commitment to data privacy and security.

Another significant control implemented at Tech Innovators Inc. to improve data security and privacy was the use of data masking. This control involved a process by which sensitive data would be converted into such format that, even if accessed by any unauthorized entity, could not easily be interpreted, yet it retained its functional properties for testing and development purposes. Data masking was implemented in support of the organization's topic-specific policy about access control and other related policies, thereby ensuring conformance to applicable legislation and business requirements. This practice was critical in mitigating several critical threats related to data loss, data exfiltration, insider threats, account compromise, and insecure interfaces with third-party systems. The masking of data by Tech Innovators Inc. decreased the risks associated with cloud adoption by rendering it meaningless to possible attackers and thus safeguarding the sensitive information processed by their AI and cloud products.

Data masking had been influential in the company's products. It allowed very secure sharing of data by Tech Innovators Inc. with users, such as testers and developers, for running secure and efficient development processes. Besides, it served as a way of sanitization in that it replaced the old values with masked values so that normal file deletion would not leave any sensitive information behind. This was particularly important for safeguarding the integrity and secrecy of personally identifiable information with their AI-based analytics platforms, which require huge amounts of data in order to tap into accurate insights. Only then could Tech Innovators Inc. continue its record of innovation and ease in products while meeting increasingly stringent data security requirements and ensuring end-user privacy.

4.4.7 Data Leakage Prevention

Implementing data leakage prevention controls at Tech Innovators Inc. represented one big step forward in their information security strategy. Understanding the huge demand and requirement for enhanced DLP solutions, the company decided to take another route: develop its own DLP tool. This decision was influenced first and foremost by the protection of sensitive data, but also by the potential to offer this tool to the market for application in addressing a rising demand related to efficient DLP solutions across several industries. Tech Innovators Inc. has assured that their own DLP tool adheres to the strict standards and guidelines of NIST and ENISA in respect of data protection, specifically those spelled out in NIST SP 800-124 Rev. 1 and SP 800-137, together with ENISA's "Procure Secure: A guide to monitoring of security service levels in cloud contracts."

These guidelines made sure that the DLP tool was designed with a view toward reaching the highest level of security standards relevant to identifying, monitoring, preventing, and tackling data leaks across the company's digital landscape.

Advanced features in the DLP tool by Tech Innovators Inc. include detection and mitigation of data leakage. It has sophisticated algorithms that monitor data flows for the identification of potential security breaches in real-time. It continuously monitors the security status of information systems and provides in-depth insights in applying principles from NIST SP 800-137. This proactive approach gives the company the chance to detect anomalies and possible data leakages very fast, minimizing the risk of data breaches. Also, integration with the guidelines in ENISA's "Procure Secure" has provided this DLP tool with special worth in a cloud computing setting by allowing security service level control across cloud contracts. It is a critical capability for protection of sensitive data stored and processed in the cloud; provides a secure cloud environment to ensure that the service provider complies with security commitments.

Soon, however, Tech Innovators Inc. plans to bring its DLP tool into the market based on an assessment for the same of the market needs in a robust data protection solution. It expected high uptake of the revolutionary DLP tool, which has already drastically improved the security of AI-powered analytics platforms and cloud computing services. By avoiding data leakage, Tech Innovators Inc. was in a position to reassure customers on matters of data privacy and security, thus boosting their trust in the Company's compliance with regulatory provisions. Continuous testing and improvement of the DLP tool are important for its long-term success in terms of maturing to respond to new threats and continuing to have relevance as a fit tool for internal use and, at a later stage, possibly even for their clients. This strategic move that Tech Innovators Inc. is involved in is intended to help more businesses improve standards of data security, thereby improving the cyber environment and solidifying their leadership in information security solutions.

4.4.8 Monitoring Activities & Web filtering

Setting up the monitoring activity and web filtering controls at Tech Innovators Inc. greatly enhanced the security and performance of their artificial intelligence-driven analytics platforms and cloud computing services. The real-time application performance monitoring would be able to trace the performance, availability, and user experience in terms of execution on a real-time basis for all its applications. This will facilitate early identification and resolution of issues, thereby ensuring that customer experience is seamless and positive. These APM tools were engaged in the optimization of applications to peak performance, thus forestalling any issues in customer service or complaints arising therefrom against a potential failure. That would have been necessary for customer satisfaction and trust, as each issue leading to downtime or degraded performance directly impacted the user's experience and company reputation.

Other areas that increased the operational efficiency for Tech Innovators Inc. are system and network monitoring activities. System monitoring also involved the use of measurable events or outputs that would identify the system's deviant behavior to expected norms for diagnosis of faults. Through continuous surveillance, all systems could be assured of working reliably and efficiently. Network activity monitoring identifies the performance of the network in real-time information, which is critical in reducing downtimes and MTTR issues.

This could let Tech Innovators Inc. easily track all activities on the network, from device status events to packet transmissions and protocol messages, in a bid to quickly identify any bottlenecks on the network and troubleshoot them before they became failures. This proactive attitude meant that configuration issues or human errors did not cause any outage; on the other hand, it provided a stable and secure network environment that would support the general health and uptime of their services. It added an important layer of protection with the controls on access to external websites, thereby reducing exposure to malicious content. In relation, this was very critical in terms of controls that avoid the company's systems' exposure to malware and block

access to unauthorized Web resources. Enforcing IT policies and preventing data leakage, web filtering ensured sensitive information is secure and confidential. This meant that the staff of Tech Innovators Inc. was safeguarded from sites that may run malicious code or pivot employee productivity. This represented a secured digital environment in the implementation of web filtering at this level by aligning internet utilization with security policies while promoting an efficient workday. In this respect, this control kept the company up to date in being compliant with concerned legislation such as CIPA (Child Internet Protection Act), which requires filtration solutions for organizations offering public internet access. Overall, the integration of monitoring activities with web filtering controls significantly improved the security, reliability, and compliance of Tech Innovators Inc.'s digital products, thus enhancing their position as a trusted provider of secure and innovative digital solutions.

4.4.9 Secure Coding

The execution of secure coding practices at Tech Innovators Inc. introduced very significant improvements in the quality and security of AI-powered analytics platforms and cloud computing services. Following up on their software development with security as an enshrined tenet that aids in lessening the potential information security vulnerabilities within its software, the company has adhered to the SSDF provided by NIST. Secure coding helps in ensuring that the security of the code squarely lies with the developers, hence instilling some culture of security awareness and accountability among the development teams. This will be informed by the left-shift security concept, which has security measures built into an early point in SDLC, hence allowing vulnerabilities identification and mitigation way before their entrenchment into the final product.

For instance, Tech Innovators Inc. followed secure-by-design principles in their development process. Every single line of code, part of their AI algorithms or cloud service interfaces, got rigorous security checks prior to committing to the code repository. This includes automated scans against vulnerabilities, adherence to coding standards, and peer reviews. By adding an abstraction layer that scans showing code and new code alike, best practices are uniformly followed to obviate human error and shortcuts in the face of tough deadlines, which are potential compromises on security. It is through this fastidiousness that the outputted software ensues not only in a robust and efficient much-anticipated version but also secure versus common threats such as SQL injection, cross-site scripting, and buffer overflow attacks.

Training has been among the most important factors in implementing secure coding at Tech Innovators Inc. The company has invested reasonably in the training programs to ensure that all its developers are knowledgeable about secure coding techniques and current security threats. They have included regular workshops, online courses, and hands-on sessions oriented toward familiarizing the developers with ways of identifying and mitigating possible vulnerabilities. It provides training to developers on secure coding and a developer's role in product security. For instance, the training will be provided to the developers of AI-powered analytics platforms on how data processing algorithms and sensitive information handled by these kinds of platforms could be secured. Similarly, those who develop into cloud services are to be trained on secure API integration and, among others, data protection in transit and at rest.

These secure coding practices have a bearing on the improved security posture of the products offered by Tech Innovators Inc. By having security baked into their development process, the risk of vulnerabilities an attacker could leverage has drastically gone down. It is not only protecting the brand image of the company but also ensures trust and confidence in the deliverables among their clientele about the security of their AI and cloud solutions. Moreover, the continued enforcement of secure coding standards has increased the overall quality and reliability of the software, reducing bugs and problems in production. Such proactive management in the security of their software places Tech Innovators Inc. at the forefront of developing secure yet innovative digital products that can safeguard against shifting landscapes in cybersecurity threats.

5. Conclusion

5.1 Summary of Findings

The thesis explained the critical role of cybersecurity standards in the certification of digital products. This research would start with a background to the basics of cybersecurity and its critical position in this age of information. It would delve deep into how robust measures in cybersecurity are put in place to protect digital infrastructures and retain trust in digital products only after basic knowledge in relation to them has been got.

Specifically, we look at key EU cybersecurity-related legal instruments: the European Cybersecurity Act and the NIS2 Directive. These have formed a significant platform in which cybersecurity standards have evolved within the European Union. The European Cybersecurity Act establishes certification frameworks, aiming to ensure a coherent system of how member states can collectively enhance the security posture of the digital products within the EU. While it is true that the purview of cybersecurity obligations under the NIS2 Directive would be expanded through further-seething areas, there are aspects regarding robust security measures against a wider scope of digital services and infrastructures. Their impact is profound in that they not only establish compliance but also best practice in adopting cybersecurity for a more secure cyber environment.

Analyses of ISO standards, notably the ISO/IEC 15408, ISO/IEC 18045, and ISO/IEC 27001:2022, shed light on structured frameworks with regard to the assessment and management of cybersecurity. ISO/IEC 15408, commonly known as Common Criteria, offers a framework that details the evaluation process for security properties in information technology products against predefined security requirements. ISO/IEC 18045 supports this with a methodology for the evaluation of IT security, guiding an evaluator through the steps of systematic assessment of security functions and assurance measures. ISO/IEC 27001:2022 is the standard on Information Security Management, detailing requirements necessary for establishing, implementing, maintaining, and continuing the improvement of an Information Security Management System. The revised 2022 version contains new controls and requirements to help deal with the evolving cybersecurity environment, equipping organizations with capabilities to manage information security risks more effectively.

The case study of an audit for an AI and ICT company according to ISO/IEC 27001:2022iligible event, showing practical applications and the flow of benefits accruing from compliance. The practice served in this exercise as an example, demonstrating a clear path toward applying controls that would improve the company's position regarding security matters. Some of the key values that benefited from this were risk management, alignment to regulatory requirements, enhanced trust with customers, and resilience against cyber-attack threats. Students specifically reported that new controls under ISO/IEC 27001:2022, especially on threat intelligence, secure coding practices, and cloud security, made a big difference. These controls dealt with existing vulnerabilities and prepared the company on impending threats so that protection of its digital products could be pursued to the end.

5.2 Future Work

Future research should aim at the orientation and probable integration of new technologies like AI and blockchain into cybersecurity standards. That will mean convergence between artificial intelligence and cybersecurity can create new security solutions by making use of the mechanisms of machine learning in threat detection and response. Blockchain technology, being a decentralized and immutable technology, offers a robust mechanism of security for digital transactions and data integrity. What would be important is how these technologies could be standardized in cybersecurity frameworks so they may be effectively adopted.

Comparative studies across these various international frameworks of cybersecurity will bring out deeper insights into global best practices. They should be able to demonstrate the strengths and weaknesses of the different approaches, thus helping in the formulation of more comprehensive standards that can apply universally. For example, comparing the EU's approach with frameworks like the NIST Cybersecurity Framework in the US or the Cybersecurity Act in Singapore might bring forth areas that would call for improvement and adaptation.

Further case studies with quantitative data will bring out a clearer picture of the practical benefit and challenges for the implementation of these standards. This will be presented more concretely if it is expressed in quantitative metrics, such as a reduction in count and criticality of security incidents after implementation, cost savings due to reduced incidents of breaches, and improvements in compliance rates. Case studies across different industries and various organizational sizes should be covered to ensure that the findings are applicable.

Bibliography

A. Pawlicka, D. J.-C. (2020). Guidelines for Stego/Malware Detection Tools: Achieving GDPR Compliance. *IEEE Technology and Society Magazine*, pp. 60-70.

A. Salih, S. T. (2021). A Survey on the Role of Artificial Intelligence, Machine Learning and Deep Learning for Cybersecurity Attack Detection. In IEEE, *2021 7th International Engineering Conference "Research & Innovation amid Global Pandemic" (IEC)* (pp. 61-66). Erbil, Iraq.

Aizuddin, A. (2001). *https://www.sans.org/white-papers/545/.* Retrieved from https://www.sans.org/white-papers/545/

al., R. N. (2020). An Interledger Blockchain Platform for Cross-Border Management of Cybersecurity Information. In IEEE, *IEEE Internet Computing* (pp. 19-29).

Ananda, S. A. (2022). Analysis Of The EU Cybersecurity Act Under The Theory Of Neoliberal Institutionalism. pp. 176–199.

Calder, A. (2018). *NIST Cybersecurity Framework: A Pocket Guide.* IT Governance Publishing.

Chen, H. B. (n.d.). A Supporting Environment for IT System Security Evaluation Based on ISO/IEC 15408 and ISO/IEC 18045. *Park, J., Stojmenovic, I., Jeong, H., Yi, G. (eds) Computer Science and its Applications. Lecture Notes in Electrical Engineering.* Berlin, Heidelberg.

D. P. F. Möller, H. V. (2022). Cybersecurity Certificate in Digital Transformation. In *2022 IEEE International Conference on Electro Information Technology (eIT)* (pp. 556-561). Mankato, MN, USA: IEEE.

Dimitra Markopoulou, V. P. (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. *Computer Law & Security Review*.

ENISA, T. D. (2006). *https://www.enisa.europa.eu.* Retrieved from https://www.enisa.europa.eu/publications/risk-management-principles-and-inventories-for-risk-management-risk-assessment-methods-and-tools

Falco, G. a. (2021). What Do I Need to Know About Cyber Frameworks, Standards, and Laws. In G. a. Falco, *Confronting Cyber Risk: An Embedded Endurance Strategy for Cybersecurity* (pp. 58-78).

Garnier, T. C. (2018). *European CEN-CENELEC Standardization on Material Efficiency for longer lifespan within Circular Economy.*

Hernández-Ramos, J. a. (2021). The Challenges of Software Cybersecurity Certification. *IEEE Security and Privacy Magazine*, 99-102.

K. Hovhannisyan, P. B. (2021). Towards a Healthcare Cybersecurity Certification Scheme. *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)* (pp. 1-9). Dublin, Ireland: IEEE.

Kohler, C. (2020). The EU Cybersecurity Act and European standards: an introduction to the role of European standardization. *International Cybersecurity Law Review*, 7-12.

Lam, M. L.-L.-W. (2021). Shared Cybersecurity Risk Management in the Industry of Medical Devices. *International Journal of Cyber-Physical Systems* , 37-56.

Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. In *Business Horizons* (pp. 659-671).

Malatji, M. (2023). Management of enterprise cyber security: A review of ISO/IEC 27001:2022. *2023 International Conference On Cyber Management And Engineering (CyMaEn)* (pp. 117-122). Bangkok, Thailand: IEEE.

Mitrakas, A. (2018). The emerging EU framework on cybersecurity certification. pp. 411-414.

Mtsweni, J. a. (2018). A unified cybersecurity framework for complex environments. *Proceedings of the Annual Conference of the South African Institute of Computer Scientists and Information Technologists* (pp. 1–9). New York, NY, USA: Association for Computing Machinery.

Najmudin Saqib, V. G. (2020). Mapping of the Security Requirements of GDPR and NISD.

OpenAI. (2024). *ChatGPT (GPT-4)*. Retrieved from https://chat.openai.com/

S. Karagiannis, M. M. (2021). Automated and On-Demand Cybersecurity Certification. In IEEE, *2021 IEEE International Conference on Cyber Security and Resilience (CSR)* (pp. 174-179). Rhodes, Greece.

Sara Degli-Esposti, E. M. (2021). After the GDPR: Cybersecurity is the Elephant in the Artificial Intelligence Room. In E. M. Sara Degli-Esposti, *European Business Law Review* (pp. 1-24).

Sara N. Matheu, J. L.-R. (2021). A Survey of Cybersecurity Certification for the Internet of Things. *A Survey of Cybersecurity Certification for the Internet of Things*, 36.

Shoemaker, D. (2015). The NICE Framework: Why You Need to Understand This Important Initiative. pp. 1-7.

Sievers, T. (2021). Proposal for a NIS directive 2.0: companies covered by the extended scope of application and their obligations. *Int. Cybersecur. Law Rev. 2*, pp. 223–231.

Skias, D. a.-H. (2022). *Demonstration of alignment of the Pan-European Cybersecurity Incidents Information Sharing Platform to Cybersecurity policy, regulatory and legislative advancements.* New York, NY, USA: Association for Computing Machinery.

Smaxwil, F. (2011). The standardization package - View of CEN-CENELEC. *2011 7th International Conference on Standardization and Innovation in Information Technology (SIIT)* (pp. 1-2). Berlin, Germany: IEEE.

Teoh, C. H. (2021). Conceptualizing Cybersecurity Management Impact on Performance: Agility and Information Technology Governance. In IEEE, *2021 IEEE International Conference on Computing (ICOCO)* (pp. 196-201). Kuala Lumpur, Malaysia.

V. Sundararajan, A. G. (2022). The Most Common Control Deficiencies in CMMC non-compliant DoD contractors. *2022 IEEE International Symposium on Technologies for Homeland Security (HST)* (pp. 1-7). Boston, MA, USA: IEEE .